UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

TEMA:

"SISTEMA DE GESTIÓN DE SEGURIDAD PERIMETRAL PARA LA RED DE DISTRIBUCIÓN Y ACCESO DE LA COOPERATIVA DE AHORRO Y CRÉDITO ESCENCIA INDÍGENA LTDA. IBARRA BASADO EN LA NORMA ISO 27002:2013"

AUTORA: KARINA ESTEFANÍA QUILCA BURGOS

DIRECTOR: ING. DIEGO TREJO

IBARRA - ECUADOR

2016

UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN

A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

La Universidad Técnica del Norte dentro del proyecto Repositorio Digital Institucional, determinó la necesidad de disponer de textos completos en formato digital con la finalidad de apoyar los procesos de investigación, docencia y extensión de la Universidad.

Por medio del presente documento dejo sentada mi voluntad de participar en este proyecto, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO	
CÉDULA DE IDENTIDAD:	1003299169
APELLIDOS Y NOMBRES:	QUILCA BURGOS KARINA ESTEFANÍA
DIRECCIÓN:	SANTA ROSA DEL TEJAR
EMAIL:	karo_keqb2890@hotmail.com
TELÉFONO FIJO:	062-650-364
TELÉFONO MÓVIL:	0996658511
DATOS DE LA OBRA	
TÍTULO:	"SISTEMA DE GESTIÓN DE SEGURIDAD PERIMETRAL PARA LA RED DE DISTRIBUCIÓN Y ACCESO DE LA COOPERATIVA DE AHORRO Y CRÉDITO ESCENCIA INDÍGENA LTDA. IBARRA, BASADO EN LA NORMA ISO 27002:2013"
AUTOR (ES):	KARINA ESTEFANÍA QUILCA BURGOS
FECHA:	ABRIL 2016
PROGRAMA:	☒ PREGRADO
TITULO POR EL QUE OPTA:	INGENIERA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN
ASESOR /DIRECTOR:	ING. DIEGO TREJO

2. AUTORIZACIÓN DE USO A FAVOR DE LA UNIVERSIDAD

Yo, Karina Estefanía Quilca Burgos, con cédula de identidad Nro. 1003299169, en calidad de autor (es) y titular (es) de los derechos patrimoniales de la obra o trabajo de grado descrito anteriormente, hago entrega del ejemplar respectivo en formato digital y autorizo a la Universidad técnica del Norte, la publicación de la obra en el Repositorio Digital Institucional y uso del archivo digital en la Biblioteca de la Universidad con fines académicos, para ampliar la disponibilidad del material y como apoyo a la educación, investigación y extensión; en concordancia con la Ley de Educación Superior Artículo 144.

3. CONSTANCIAS

El autor manifiesta que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto la obra es original y que es el titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de la misma y saldrá en defensa de la universidad en caso de reclamación por parte de terceros.

.....

Firma

Nombre: Karina Estefanía Quilca Burgos

Cédula: 100329916-9

Ibarra, Abril del 2016

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE GRADO A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

Yo, Karina Estefanía Quilca Burgos, con cédula de identidad Nro. 1003299169, manifiesto mi voluntad de ceder a la Universidad Técnica del Norte los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autor (es) de la obra o trabajo de grado denominado: "**SISTEMA DE GESTIÓN DE SEGURIDAD PERIMETRAL PARA LA RED DE DISTRIBUCIÓN Y ACCESO DE LA COOPERATIVA DE AHORRO Y CRÉDITO ESCENCIA INDÍGENA LTDA. IBARRA, BASADO EN LA NORMA ISO 27002:2013** ", que ha sido desarrollado para optar por el título de Ingeniera en Electrónica y Redes de Comunicación en la Universidad Técnica del Norte, quedando la Universidad facultada para ejercer plenamente los derechos morales de la obra antes citada. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Técnica del Norte.

.....

Firma

Nombre: Karina Estefanía Quilca Burgos

Cédula: 100329916-9

Ibarra, Abril del 2016

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CERTIFICACIÓN

Certifico que bajo mi dirección el trabajo de grado: "**SISTEMA DE GESTIÓN DE SEGURIDAD PERIMETRAL PARA LA RED DE DISTRIBUCIÓN Y ACCESO DE LA COOPERATIVA DE AHORRO Y CRÉDITO ESCENCIA INDÍGENA LTDA. IBARRA, BASADO EN LA NORMA ISO 27002:2013**", fue desarrollado en su totalidad por la señorita estudiante Quilca Burgos Karina Estefanía, previo a la obtención del título de Ingeniera en Electrónica y Redes de Comunicación.

Por lo expuesto:

Autorizo su presentación ante los organismos competentes para sustentación del mismo.

Ing. Diego Trejo

DIRECTOR DE TESIS

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

DECLARACIÓN

Yo, Karina Estefanía Quilca Burgos, con cédula de identidad Nro. 1003299169, declaro bajo juramento que el trabajo aquí descrito es de mi autoría, que no ha sido previamente presentado para ningún grado o calificación profesional, y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo los derechos de propiedad intelectual correspondiente a este trabajo, a la Universidad Técnica del Norte, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y por la normatividad institucional vigente.

.....

Firma

Nombre: Karina Estefanía Quilca Burgos

Cédula: 100329916-9

Ibarra, Abril del 2016

DEDICATORIA

Dedico este proyecto final de graduación, en primera instancia al Todopoderoso quien me ha dado la fortaleza suficiente para poder seguir adelante, inclusive en los momentos más difíciles, cuando he estado a punto de caer él me ha dado la fortaleza para continuar; a mis padres: Luis Enrique Quilca Ipiales, Marina Olivia Burgos Nicaragua y hermanas: Vero, Erika, Tatys quienes siempre han sido un ejemplo en mi vida, que con su amor, apoyo y preocupación han estado a mi lado siempre. Y por último pero no menos importante, a Diego quien ha estado, siempre inquebrantable a mi lado, dándome todo su apoyo, comprensión y cariño, alguien que le da a la palabra amor y compañía un nuevo significado.

Karina Estefanía Quilca Burgos

AGRADECIMIENTO

Agradezco de manera muy especial al Ing. Diego Trejo por su dirección y consejos en la realización del presente proyecto; además a los profesores de la Universidad Técnica del Norte ya que contribuyen a la formación de personas integras las cuales constituyen una parte importante de la sociedad.

También expreso mi agradecimiento a la Cooperativa de Ahorro y Crédito Escencia Indígena Ltda. Por la apertura y atención brindada durante todo este proceso.

Karina Estefanía Quilca Burgos

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

Este proyecto presenta un sistema de gestión de seguridad perimetral para la red de distribución y acceso de la cooperativa de ahorro y crédito Escencia Indígena ltda. Ibarra, basado en la norma ISO 27002:2013.

Se inició con la fundamentación teórica de los temas de seguridad de la información, ataques informáticos, métodos y herramientas para combatirlos. Se visitó la institución con el fin de identificar su infraestructura tecnológica, identificar riesgos y vulnerabilidades y encontrar una solución.

Se realizó el manual de políticas y buenas prácticas de seguridad de la información en base a los objetivos de control y controles de la norma ISO/IEC 27002:2013 aplicables a los problemas y necesidades encontrados en la infraestructura tecnológica tanto a nivel de usuarios finales y en la capa de distribución de la institución.

Se adquirió e instaló un equipo gateprotect GPA 500 que reúne todas las características para el diseño planteado y contempla un firewall, DMZ e IDS/IPS además de otras características como control de spam, virus y otros,

Finalmente se realizó el análisis de costos de los equipos que se utiliza en el diseño planteado con el fin de conocer la inversión del proyecto. También se redactó las conclusiones y recomendaciones obtenidas en el desarrollo del proyecto.

SUMMARY

This project presents a management system for perimeter security and access distribution network of the saving and credits Cooperative Escencia Indígena Ltda. Ibarra, based on the ISO 27002:2013 norm.

It was started with the theoretical Foundation related with the themes about information security, cyber-attacks, methods and tools to combat them. The institution was visited in order to identify its technology infrastructure, identify risks and vulnerabilities, and find a solution.

The handbook of policies and good practices of information security was made based on Objectives controls and checkpoint of the ISO / IEC 27002: 2013 applicable to the problems and needs found in the technological infrastructure at last users level and in the distribution layer of the institution.

An equipment Gate Protect GPA 500 was purchased and installed because it has all the features for the proposed design and includes a firewall, DMZ and IDS / IPS, moreover of features such as spam controlling, viruses and others.

Finally, the analysis of the cost of equipment that used in the design was made in order to know the project investment. Also, the conclusions and recommendations obtained in the project was written.

PRESENTACIÓN

El presente proyecto permite resguardar la infraestructura tecnológica de la Cooperativa de Ahorro y Crédito Escencia Indígena mediante la implementación de un sistema de seguridad perimetral que incluye un firewall, una zona desmilitarizada, un detector de intrusos configurados en el equipo Gateprotect GPA 500 el cual además de estas funciones ofrece otras bondades como el control de virus, spam, gestión de la red. Completando con un manual de políticas y buenas practicas dirigido a todos los funcionarios de la misma mejorando de esta manera la forma de actuar hacia los equipos e infraestructura de la empresa.

CAPÍTULO I

1 ANTECEDENTES

La Cooperativa de ahorro y crédito Escencia Indígena es una empresa financiera de carácter privada creada por un grupo de personas emprendedoras de la provincia de Imbabura y Tungurahua el 19 de mayo del 2007. Dispone de un grupo de servidores (base de datos, ventanilla móvil, facilito, APP ventanillas, intranet, etc. Ubicados en la agencia Ibarra la cual se desempeña como matriz y desde allí se distribuyen y controlan los servicios y aplicaciones al resto de agencias ubicadas en las distintas ciudades del país. (Castañeda, 2013b).

1.1 PROBLEMA

Utiliza el proveedor CNT para brindar el servicio de internet y para la interconexión entre la matriz y las sucursales en: Otavalo, Tulcán, Ambato, Cañar, Azogues, Salcedo y Ambato Huachi; para Cuenca y Quito se trabaja con TELCONET. Existen diferentes perfiles de usuarios con sus respectivas claves y niveles de acceso a las diferentes aplicaciones lo cual evita la manipulación de personas no autorizadas, sin embargo, este proceso no es muy confiable ya que en varias ocasiones los usuarios olvidan su contraseña y bloquean su usuario o la configuración de sus perfiles no contienen los permisos a todas las actividades que deben realizar lo cual genera demora en la atención a los clientes. El acceso al cuarto de equipos de telecomunicaciones y su ambiente no es el adecuado ya que no existe un control de acceso y allí se almacenan otros activos diferentes a los de un cuarto de telecomunicaciones.

Por este motivo con el desarrollo de este trabajo, la aplicación de la norma de seguridad ISO/IEC 27002:2013 y concientizando a sus colaboradores al manejo de buenas prácticas de seguridad se quiere reducir la probabilidad de ocurrencia de los riegos a los que se ven expuestos y que están afectando a los activos de la cooperativa. Se deberá tomar en cuenta que los servidores tengan instalados solamente el software necesario para cumplir con su función evitando que se instale software malicioso cuyo objetivo es dañarlos o dar la oportunidad a los hackers que se apoderen de información confidencial de la empresa.

Mediante su desarrollo se desea contribuir al crecimiento de la cooperativa al utilizar mecanismos de protección de información y servicios más robustos que beneficien a los socios, personal administrativo y clientes, al garantizar la confiabilidad de la información que se maneja como saldos y transacciones evitando modificaciones y fraudes en las cuentas de ahorro y cuentas corrientes.

1.2 OBJETIVOS DEL PROYECTO

1.2.1 OBJETIVO GENERAL

Diseñar e implementar un sistema de gestión de seguridad perimetral para la cooperativa Escencia Indígena, en base a políticas y buenas prácticas de la norma ISO/IEC 27002:2013 y procedimientos de seguridad para evitar ataques internos y externos a la red.

1.2.2 OBJETIVOS ESPECÍFICOS

- Fundamentar teóricamente los temas relacionados a la seguridad de la información y las soluciones existentes para comprender mejor y diseñar la solución más adecuada.
- Identificar la infraestructura tecnológica actual de la cooperativa con el fin de detectar y evaluar los riesgos y vulnerabilidades encontrados expresando los impactos que estos ocasionan en el desempeño de las actividades y funciones de la empresa.
- Establecer políticas y procedimientos de seguridad de la información en base a los riesgos encontrados en la infraestructura tecnológica de la cooperativa y la norma ISO/IEC 27002:2013.
- Diseñar el sistema de aseguramiento perimetral aplicando la norma ISO/IEC27002:2013, herramientas y procedimientos adecuados.
- Analizar diferentes plataformas de Hardware y Software en base al estándar IEEE 830 de especificaciones de requerimiento de software para elegir la alternativa que mejor se ajuste a los requerimientos del diseño planteado.
- Implementar la DMZ, firewall e IDS con las respectivas políticas de seguridad establecidas con anterioridad.
- Realizar pruebas de funcionamiento mediante procedimientos que simulen ataques internos y externos a la red.
- Realizar un análisis de costos de los equipos que se usarán para el diseño planteado.

1.3 JUSTIFICACIÓN

El desarrollo de este proyecto mediante la investigación de las mejores prácticas y procedimientos de seguridad de la información para la infraestructura tecnológica de la cooperativa de ahorro y crédito Escencia Indígena cumple con los criterios de incentivación a la investigación, sustentabilidad, desarrollo social y económico del país como se menciona en la misión de la Universidad Técnica del Norte.

Se plantea el diseño de una solución que satisfaga las expectativas de la cooperativa mediante la prestación de servicios financieros a los sectores productivos y comunidad en general de una forma eficiente, transparente y con total credibilidad; asegurando que solo personas autorizadas tengan acceso a la información, que la información y los procesos son los reales y estén disponibles cuando los clientes lo necesiten lo cual da mayor valor a su reputación y continuidad del negocio (Castañeda, 2013).

Para el desarrollo de este proyecto se ha decidido utilizar las políticas de seguridad descritas en los diferentes objetivos de control y controles de la norma ISO/IEC 27002:2013 las cuales son más claras y se las aplicará en el ámbito de la seguridad a nivel de red de distribución y acceso debido a que la mayoría de modelos de seguridad se enfocan a mantener solamente las amenazas externas lejos de la organización pero muchas veces los riesgos más potenciales se generan dentro de la red. Por esta razón se considerarán los dos niveles.

Finalmente, aparte del aporte técnico y social, este proyecto tiene gran impacto personal ya que me permite poner en practica la investigación y aplicar los conocimientos adquiridos durante la formación de la carrera dándome la oportunidad de optar por la titulación al finalizar este proceso y de igual forma incentiva a seguir investigando y encontrar nuevas y mejores formas para desarrollarlo en el campo profesional.

1.4 ALCANCE

El presente proyecto plantea proteger la infraestructura tecnológica de la cooperativa de ahorro y crédito Escencia Indígena a nivel de distribución y datos mediante la utilización de herramientas detectoras de intrusos y la aplicación de políticas y buenas prácticas de seguridad tomando como referencia la norma ISO/IEC 27002:2013, además del cumplimiento de la ley de la Superintendencia de Bancos y Seguros y la ley de Cooperativas de Ahorro y Crédito en lo referente a seguridad de la información.

Para ello se empezará con la fundamentación teórica de los temas de seguridad de la información, ataques informáticos, métodos y herramientas para combatirlos, normas de seguridad y demás temas afines con el fin de tener claro la problemática y la solución a desarrollar recurriendo a la investigación en textos, revistas, internet, tesis afines y demás documentos válidos.

Se visitará la institución con el fin de identificar su infraestructura tecnológica, determinando: su diseño, activos que posee con su debido grado de importancia y utilidad, los servicios que ofrece a la ciudadanía Ibarreña y el país en general en base a las aplicaciones que dispone. Se identificarán los riesgos y vulnerabilidades que afronta actualmente la cooperativa, se evaluará el impacto que estos generan en el desempeño y cumplimiento de la función principal y se buscará la forma de solucionarlos.

Posteriormente se establecerán las políticas y buenas prácticas de seguridad de la información en base a los objetivos de control y controles de la norma ISO/IEC 27002:2013 aplicables a los problemas y necesidades encontrados en la infraestructura tecnológica tanto a nivel de usuarios finales como en la capa de distribución de la institución; considerando también las exigencias de ley de la Superintendencia de Bancos y Seguros y la ley de Cooperativas de Ahorro y Crédito en lo que se refiere a seguridad de la información y transparencia de sus servicios.

En base a los resultados obtenidos del análisis y evaluación de los riesgos que se desarrollará con anterioridad se procederá a diseñar el sistema de aseguramiento perimetral que ayude a disminuir los principales riesgos contra los activos más importantes de la cooperativa, el cual contemplará la implementación de un firewall a nivel de hardware, una red DMZ, sistemas de detección de intrusos (IDS) y otros procedimientos que se determinen necesarios al analizar los riegos de la empresa.

Se utilizará el estándar IEEE 830 para establecer los parámetros y requerimientos con los que debe cumplir el software que se empleará en el sistema de seguridad de igual manera para el hardware se realizará una comparación de al menos 2 fabricantes de estas soluciones y de esa manera elegir los más adecuados.

El firewall permitirá el acceso desde el internet hacia la red local a los servicios web y correo electrónico, como también se controlará el acceso a través de la red local hacia el internet dependiendo de los departamentos y sus funciones.

Se realizará una zona desmilitarizada DMZ que permitirá acceder solo personal autorizado a los servidores como: servidores de correo electrónico, Web, DNS, Servidor Facilito, servidor de base de datos, ventanillas móviles, servidor de aplicación y demás servidores con los que trabaja la empresa.

Se implementará el IDS para prevenir ataques de intrusos y como complemento del firewall. Posterior a ello, se llevará a cabo las pruebas de funcionamiento mediante el escaneo de puertos, denegación de servicios en uno o varios recursos críticos para descubrir las vulnerabilidades y fallos de la seguridad que se presenten. Finalmente se realizará un análisis de costos de los equipos que se van utilizar en el diseño planteado con el fin de conocer la inversión que este tendrá.

CAPÍTULO II

2 MARCO TEÓRICO

En este capítulo se presenta la fundamentación teórica necesaria para el entendimiento del problema que se desea solucionar; se detallará los conceptos de seguridad de la información, ataques informáticos, métodos y herramientas para combatirlos además de las normas de seguridad de la información dando mayor realce a la ISO/IEC 27002:2013

2.1 CONCEPTOS BÁSICOS DE SEGURIDAD EN REDES

Antes de plantear una solución a este problema es necesario tener claro ciertos conceptos que conlleva la seguridad en redes, tales como información, redes de datos, amenazas, vulnerabilidades, políticas, métodos y herramientas para combatir ataques indeseados. A continuación, algunos de ellos.

2.1.1 INFORMACIÓN

La información dentro de una institución o empresa constituye uno de los activos más importantes que poseen, por lo que es necesario emplear diferentes controles de seguridad que garanticen la operatividad y continuidad del negocio.

2.1.2 SEGURIDAD DE LA INFORMACIÓN

Resguardar la información y la integridad de un sistema informático es un factor muy importante para una empresa u organización para evitar pérdidas económicas e información confidencial.

Por lo indicado anteriormente se considera muy importante la seguridad informática, y se define como un conjunto de procedimientos, dispositivos y herramientas encargadas de asegurar la integridad, disponibilidad y privacidad de la información en un sistema informático e intentar reducir las amenazas que pueden afectar al mismo (García, Hurtado, & Alegre, 2011).

2.2 IDENTIFICACIÓN DE RIEGOS

Proceso por el cual se identifica y cuantifica la probabilidad de que se produzcan amenazas.

2.2.1 AMENAZAS EN LA SEGURIDAD DE LA INFORMACIÓN

Las amenazas informáticas son acciones realizadas por programas maliciosos o intrusiones de individuos no autorizados con el fin de alterar el correcto funcionamiento de una red.

2.2.2 CLASIFICACIÓN

Se puede encontrar diferentes clasificaciones dependiendo del autor que se considere, en la **FIGURA 2. 1:** se muestra una de ellas.

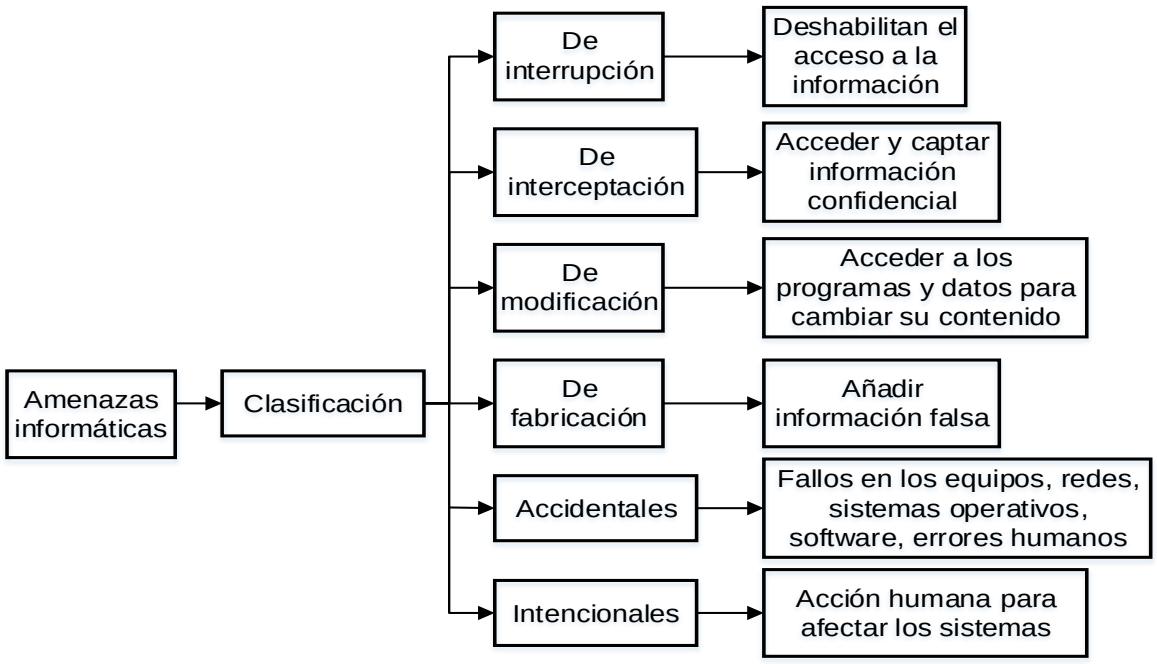


FIGURA 2. 1: Clasificación de amenazas de la información.
Fuente: Desarrollo del proyecto

2.2.3 VULNERABILIDADES EN LA SEGURIDAD DE LA INFORMACIÓN

Una vulnerabilidad es un punto débil que por sí mismo no causa ningún daño, pero al ser explotado por amenazas afectan la confidencialidad, disponibilidad e integridad de la información de una persona o una empresa.

Las vulnerabilidades se pueden clasificar de diferentes maneras tal como se muestran en la **FIGURA 2. 2**

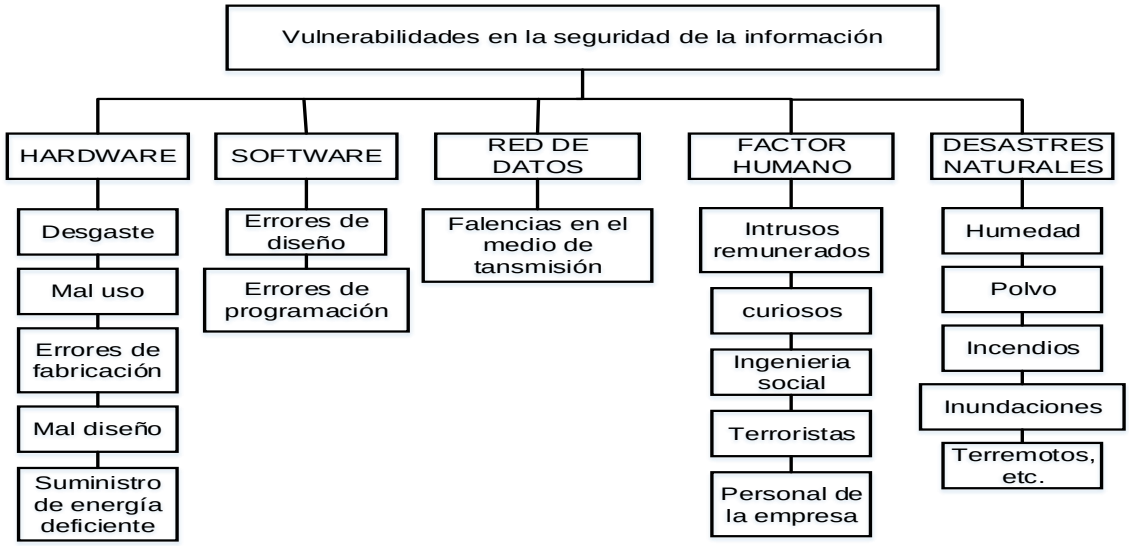


FIGURA 2. 2: Clasificación de vulnerabilidades en la seguridad de la información.

Fuente: Desarrollo del proyecto

2.2.4 ATAQUES A LA SEGURIDAD DE LA INFORMACIÓN

Un ataque informático es un método por el cual un individuo, mediante un sistema informático, intenta tomar el control, desestabilizar o dañar otro sistema informático. Existen diferentes tipos de ataques informáticos en la **FIGURA 2. 3** se presentan algunos de ellos.

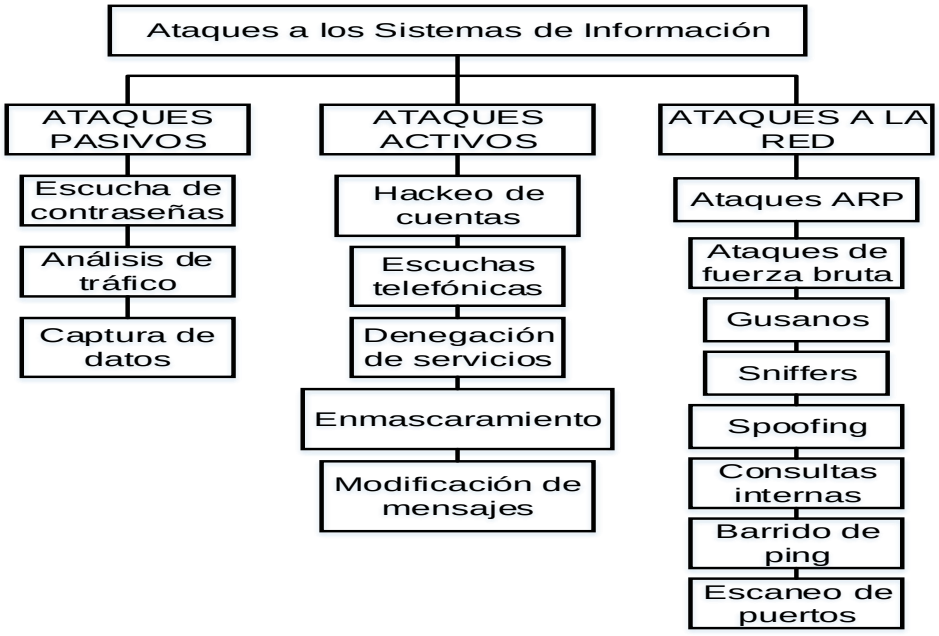


FIGURA 2. 3: Tipos de ataques informáticos.

Fuente: Desarrollo del proyecto

2.2.5 REQUISITOS PARA LA SEGURIDAD INFORMÁTICA

Entre los requisitos necesarios para establecer seguridad en una red se encuentran:

- **Confidencialidad. -** protección de la información ante accesos no autorizados.

- **Integridad.** enfocada a la exactitud de los datos; se los protege de alteraciones no autorizadas, no controladas u ocasionadas accidentalmente no solo en su trayecto sino también en el origen.

- **Disponibilidad.-** se refiere a que todos los elementos que componen el sistema puedan recuperarse rápida y completamente ante una interrupción inesperada.

- **Autenticación.-** garantiza que un usuario es quien dice ser mediante su autenticación y registro.

2.3 SEGURIDAD PERIMETRAL

Las redes de comunicación de cualquier empresa o entidad están expuestas a ataques cibernéticos debido a que están conectados a internet; estos ataques son realizados con la intención de acceder a información confidencial, denegar servicios o definitivamente paralizar la red ocasionando desprestigio y grandes pérdidas económicas. Por esta razón es importante utilizar métodos de seguridad para evitar estos ataques, tal es el caso de la seguridad perimetral que se encarga de controlar y verificar el flujo entrante y saliente de una red.

2.3.1 CONCEPTO DE SEGURIDAD PERIMETRAL

“La seguridad perimetral es uno de los métodos posibles de defensa de una red, basado en el establecimiento de recursos de seguridad en el perímetro externo de la red y a diferentes niveles” (Guijarro, 2012, pág. 7). La seguridad perimetral integra elementos y sistemas, tanto electrónicos como mecánicos, para detectar y proteger a la red de intrusiones y/o amenazas.

2.3.2 OBJETIVOS DE LA SEGURIDAD PERIMETRAL

Entre los principales objetivos o metas que se tiene al aplicar seguridad perimetral en una red se determina:

- Controlar de tráfico de red desde y a hacia Internet.
- Controlar el acceso a internet de los usuarios con el fin de evitar que se visiten sitios de ocio o que contengan virus.
- Permitir conexión con equipos remotos (portátiles y dispositivos móviles)
- Gestionar el ancho de banda de internet dependiendo de la actividad que realice.
- Disponer de un sistema de Detección de Intrusos.

2.4 TECNOLOGÍAS DE SEGURIDAD PERIMETRAL

En esta sección se enlistan los métodos más utilizados para hacer frente a las amenazas mencionadas con anterioridad.

2.4.1 ENCRIPTACIÓN

Encriptar es una manera de codificar la información y hacerla irreconocible a todos aquellos usuarios no autorizados de un sistema informático de tal manera que solo los propietarios legítimos puedan recuperar la información original a través de un software o una clave secreta; esto garantiza la confidencialidad, integridad y autenticidad de los mensajes o archivos que viajan por la red.

2.4.1.1 ENCRIPTACIÓN SIMÉTRICA

Es un sistema para encriptación que utiliza una clave secreta, las partes que participan en el intercambio de información comparten el mismo algoritmo y clave secreta. La misma clave es utilizada para encriptar y des encriptar. En la **FIGURA 2. 4** se presenta este modelo.

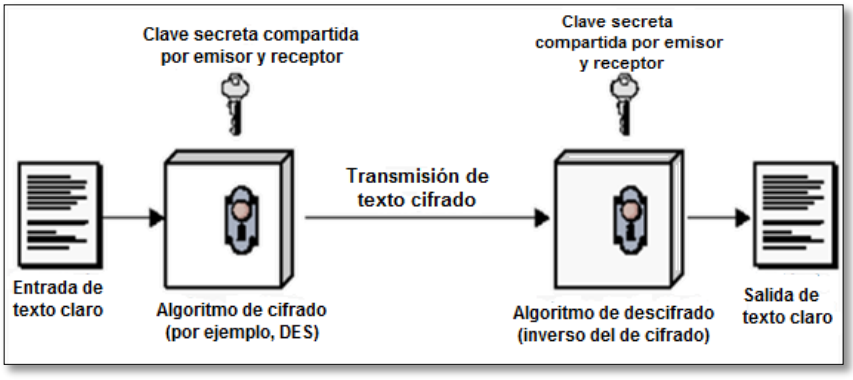


FIGURA 2. 4: Modelo simplificado del cifrado convencional

Fuente: https://morenojhonny.wordpress.com/2012/06/14/4-1-cifrado-simetrico-y-confidencialidad-de-mensajes/

2.4.1.2 ENCRIPTACIÓN ASIMÉTRICA

Es un sistema para encriptación que emplea una clave pública y una privada. Un mensaje cifrado con la clave privada solo puede ser descifrado con la correspondiente clave pública e inversamente un mensaje cifrado con la clave pública solo puede ser descifrado con la respectiva clave privada. Una clave no se deriva de la otra lo que hace más lento el proceso que un cifrado simétrico.

2.4.2 FIREWALLS

Son dispositivos de software o hardware en el que pasa todo el tráfico de entrada y salida de la red, y dependiendo de las políticas de seguridad se encarga de denegar o permitir el paso de la información.

2.4.3 ADMINISTRACIÓN DE CUENTAS

Es el medio en que todos los usuarios seguros, tienen su usuario y contraseña para acceder a los recursos de la red, este tipo de seguridad es muy susceptible a la ingeniería social por lo que es recomendable utilizar contraseñas robustas.

2.4.4 DETECCIÓN Y PREVENCIÓN DE INTRUSOS

El método de detección de intrusos es aquel que detecta al usuario o usuarios que ingresan de forma no autorizada a la red, y los bloquea en caso que sea determinado como un intruso.

2.4.5 ACCESO REMOTO

Este método sirve para poder acceder a hosts y servicios desde cualquier parte dentro y fuera de la red, de manera segura debido a que solo quien conozca la contraseña podrá ingresar al servidor de acceso remoto.

2.4.6 ANTIVIRUS

Programas informáticos especializados en la detección y eliminación de malware existente dentro de un equipo o host, aunque son muy efectivos para determinados malware, no todos los antivirus pueden eliminarlos por completo.

2.4.7 BIOMETRÍA

Es un método de control de acceso de usuarios muy efectivo, debido a que las claves para el ingreso generalmente son huellas dactilares, retina de los ojos o la voz, los cuales son únicos de cada persona.

2.4.8 FIRMA DIGITAL

Esquemas matemáticos enviados junto a un archivo o documento, los cuales permiten indicar la autenticidad del emisor.

2.5 COMPONENTES DEL SISTEMA DE GESTIÓN DE SEGURIDAD PERIMETRAL

Entre los principales mecanismos utilizados para brindar seguridad perimetral se encuentran.

2.5.1 FIREWALL

Es un conjunto de componentes hardware y software destinados a establecer controles de seguridad en el punto o puntos de entrada a una red. Separando la red interna de la red externa, está ubicado en el límite entre el espacio protegido llamado perímetro de seguridad y la red externa llamada zona de riesgo, permite o bloquea tráfico de entrada y salida en base a una serie de reglas. Su complejidad reside en las reglas que admite y en como realizan la toma de decisiones en base a dichas reglas.

Configurados de manera correcta, se convierten en dispositivos de seguridad indispensables. Sin embargo no evitará que un atacante utilice una conexión permitida para atentar contra el sistema o de un usuario interno que hace uso de la red. En la **FIGURA 2. 5** se muestra su estructura.

FIGURA 2. 5: Firewall

Fuente: Recuperado de http://www.mmbfuture.tk/2015/03/blog-post_53.html

2.5.1.1 DISEÑO Y CONFIGURACIÓN

Entre las características a tomar en cuenta al momento de implementar un firewall se encuentran:

- Políticas de seguridad de la organización.
- Nivel de monitoreo, redundancia y control.
- Aspecto económico.

2.5.1.2 COMPONENTES

A continuación se describe los componentes que hacen posible o en los que se basa el correcto funcionamiento de un Firewall.

2.5.1.2.1 FILTRADO DE PAQUETES

Se utiliza para implementar distintas políticas de seguridad, el objetivo es impedir el acceso no autorizado entre dos redes y permitir los autorizados. El funcionamiento consiste en analizar la cabecera de cada paquete generalmente en capa 3 y algunas características del tráfico generado en las capas 1, 2 y/o 4 y en función de las reglas establecidas la trama es bloqueada o se le permite continuar a su destino.

Los elementos que determinan si un paquete es válido o no son los siguientes:

- Las direcciones fuente y destino (capa 3).
- El protocolo utilizado (capas 2 y 3).
- El tipo de tráfico: TCP, UDP, ICMP, etc. (capas 3 y 4).
- El puerto destino (capa 4).
- Interfaz del router: arribo/reenvío (capa 1).

Las reglas se expresan como una tabla de condiciones y acciones que deben listarse en orden ya que de eso influirá en la toma de decisiones sobre el bloqueo o reenvío de la trama, lo cual determinará la correcta funcionalidad del firewall.

2.5.1.2.2 SERVIDOR PROXY

El proxy es un software que se ejecuta en el firewall (también puede funcionar sin un firewall) para permitir la comunicación entre dos redes de manera controlada. Las principales funciones de un proxy son: proxy- cache y proxy control parental.

Proxy cache. Permite mostrar rápidamente las páginas web, debido a los permisos de guardada de web; esto hace que la próxima vez que se visiten las páginas web no se extraerá información de la web si no que se recuperará información de la caché.

Control parental. Se encarga de permitir o no, la visualización de páginas web dependiendo de su dirección web o contenido.

Existen proxy a nivel de aplicación y a nivel de circuito.

Proxy a nivel de aplicación. Es un software utilizado para bloquear o reenviar conexiones a servicios como telnet, http o ftp; el equipo donde se ejecutan las aplicaciones se denomina pasarela de aplicación.

Proxy a nivel circuito. Crea un circuito entre un cliente y un servidor sin interpretar el origen de la petición pero requiere que el cliente ejecute una aplicación especial (SOCKS[1]).

2.5.1.2.3 MONITOREO DE LA ACTIVIDAD

Esta actividad es algo indispensable en la seguridad del perímetro protegido, ya que esto mostrará información de los intentos de ataque o de tramas sospechosas. La información que se registra es:

- Tipo de paquete recibido.
- Frecuencias.
- Direcciones fuente y destino.
- Nombre de usuario.
- Hora y duración.
- Intentos de uso de protocolos denegados.
- Intentos de falsificación de dirección.
- Tramas recibidas desde routers desconocidos.

[1] SOCKS.- es un protocolo de Internet que presenta un tipo de servidor proxy especial. Su puerto por defecto es el 1080. Funciona como una puerta de entrada a nivel de circuito, cifra los datos que pasan entre el cliente y el proxy.

2.5.1.3 ARQUITECTURAS

Es importante conocer que existen diferentes formas de ubicación del firewall, para ello a continuación se describen algunas de sus arquitecturas.

2.5.1.3.1 SCREENED ROUTER (ROUTER APANTALLADO)

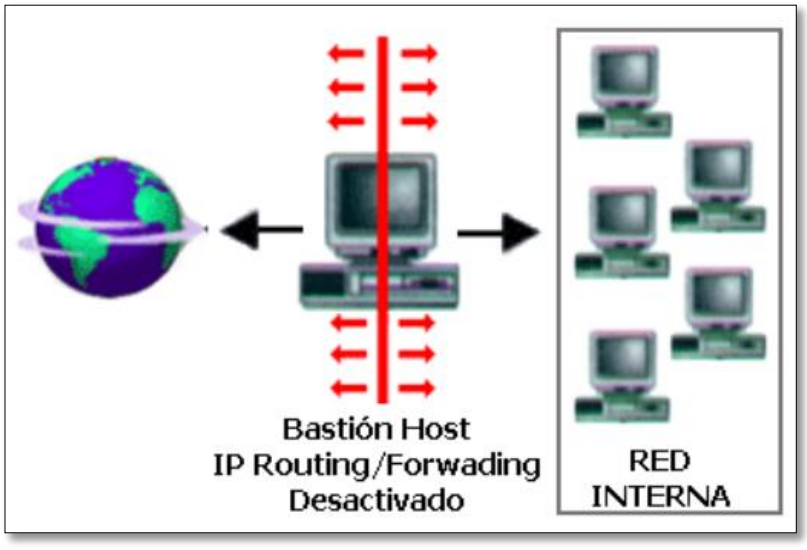
Se utiliza un router como filtro de paquetes aprovechando el enrutamiento selectivo para bloquear o permitir el flujo de paquetes mediante listas de control de acceso en función de ciertas características de las tramas.

2.5.1.3.2 HOST BASTION (SERVIDOR BASTIÓN O PASARELA DE APLICACIONES)

Es el sistema de red que se expone a la red externa y es usado para defender la red interna, ya que su función es permitir o no permitir el paso de tráfico.

2.5.1.3.3 DUAL-HOMED HOST (SERVIDOR DE DOS BASES)

Consiste en emplear una máquina con al menos dos tarjetas de red en las que una de ellas se conecta a la red interna y la otra a la externa. El sistema de la máquina ejecutará servicios proxy para cada uno de los protocolos que se permita pasar a través del firewall, véase la **FIGURA 2. 6**



.

FIGURA 2. 6: Arquitectura Dual-Homed Host

Fuente: Guijarro, Á. P. (2012). Seguridad Perimetral.

2.5.1.3.4 SCREENED HOST (SERVIDOR APANTALLADO)

La arquitectura screened host o choke-gate, que combina un router con un host bastión, y donde el principal nivel de seguridad proviene del filtrado de paquetes (es decir, el router es la primera y más importante línea de defensa).

En la máquina bastión, único sistema accesible desde el exterior, se ejecutan los proxies de las aplicaciones, mientras que el choque se encarga de filtrar los paquetes que se puedan considerar peligrosos para la seguridad de la red interna, permitiendo únicamente la comunicación con un reducido número de servicios (Guijarro, 2012). En esta arquitectura se recomienda situar el router entre la red exterior y el host bastión con la finalidad de que:

- El choke permita la salida de algunos servicios a todas o a parte de las máquinas internas a través de un simple filtrado de paquetes.

- El choke prohiba todo el tráfico entre máquinas de la red interna y el exterior, permitiendo sólo la salida de ciertos servicios que provienen de la máquina bastión y que han sido autorizados por la política de seguridad de la organización. Véase la **FIGURA 2. 7**

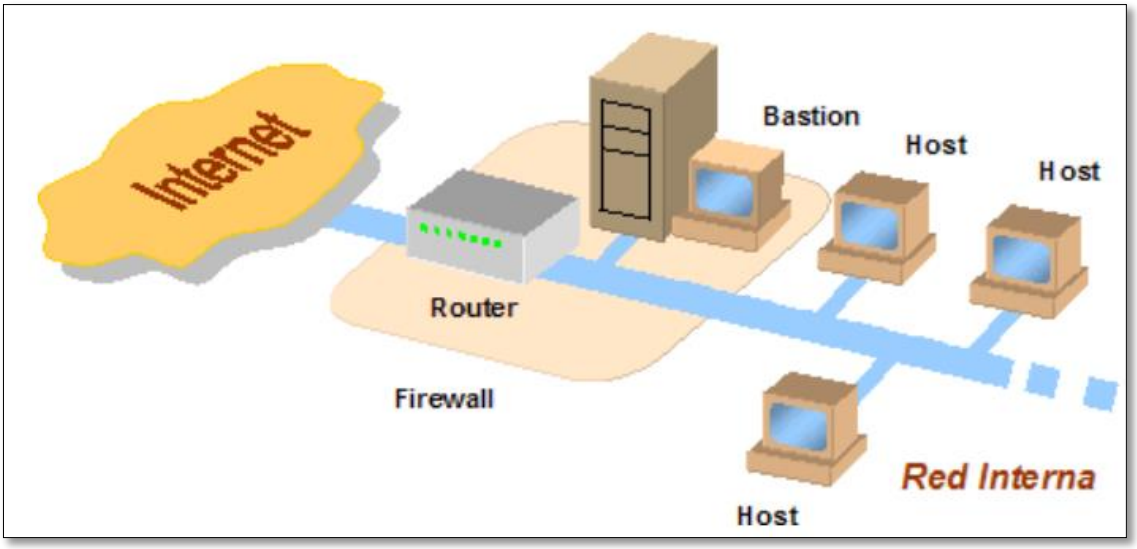


FIGURA 2. 7: Estructura Screened Host

Fuente: Guijarro, Á. P. (2012). *Seguridad Perimetral*.

2.5.1.3.5 SCREENED SUBNET (RED PERIMÉTRICA)

Consiste en situar una subred (DMZ[2]) entre la red externa y la red interna con el objeto de reducir los ataques exitosos al host bastión, éste es aislado en una red perimétrica de forma que un intruso que accede a esta máquina no consiga tener acceso total a la subred protegida.

La red perimétrica contiene al host bastión y también se puede incluir sistemas que necesiten un acceso controlado, como módems, servidor web o servidor de correo, que serán los únicos elementos visibles desde fuera de la red.

El router exterior tiene como misión bloquear el tráfico no deseado en ambos sentidos, mientras que el interior hace lo mismo pero con el tráfico entre la red interna y la perimétrica. En la **FIGURA 2. 8** se muestra la estructura de esta arquitectura.

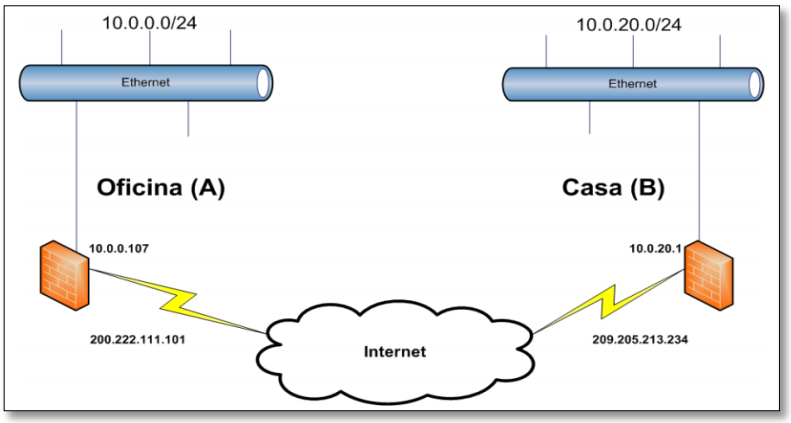


FIGURA 2. 8: Estructura Screened subnet
Fuente: Guijarro, Á. P. (2012). *Seguridad Perimetral*.

2.5.1.4 BENEFICIOS DE UN FIREWALL

- Ayuda a simplificar los trabajos de administración, una vez que se consolida la seguridad en el sistema firewall, es mejor que distribuirla en cada uno de los servidores que integran la red privada.

- Ofrece un punto donde la seguridad puede ser monitoreada y alertar en caso de presencia de intrusos.

[2] DMZ.- Demilitarized Zone (Zona desmilitarizada) es una zona segura que se ubica entre la red interna de una organización y una red externa, generalmente en Internet.

2.5.1.5 LIMITANTES DE UN FIREWALL

No se debe olvidar que el firewall es el punto de entrada a la red a proteger, pero hay amenazas contra las que un firewall no puede hacer nada y se detallan a continuación:

- Un firewall no puede proteger contra amenazas que no pasan a través de él. Por tal razón el firewall debe de ser el punto único e ineludible de acceso a la red interna. Si esto no se cumple su efectividad es parcial.
- No puede proteger contra amenazas que se producen en el interior de la red interna.
- No dan protección contra clientes o servicios que se admiten como válidos pero que son vulnerables.
- No pueden ni deben suplantar otros mecanismos de seguridad que se empleen dependiendo de la naturaleza y efectos de los datos y aplicaciones que se utilicen.

2.5.2 SISTEMAS DE DETECCIÓN DE INTRUSOS (IDS)

Constituyen sistemas administradores competentes que auditan y monitorean continuamente los sistemas en busca de intrusiones. La detección de intrusos es el arte de detectar actividades no autorizadas, inapropiadas o extrañas. Son capaces de detectar ataques en progreso, generar alarmas en tiempo real y contrarrestar un ataque mediante el lanzamiento de un evento o reconfiguración del router o firewall.

2.5.2.1 SISTEMA DE DETECCIÓN DE INTRUSOS PARA HOST (HIDS)

Habita en el host y es capaz de monitorear y negar servicios automáticamente si una actividad sospechosa es detectada; utilizan log y agentes de auditoria del sistema para el monitoreo.

Verificadores de integridad del sistema (SIV). Es un mecanismo encargado de monitorear archivos de una máquina en busca de posibles modificaciones no autorizadas.

Monitores de registro (LFM). Monitorean los archivos de log generados por los programas de una máquina en busca de patrones que indiquen un ataque o intrusión.

Sistemas de decepción. Son mecanismos encargados de simular servicios con problemas de seguridad de forma que un pirata piense que realmente el problema se puede aprovechar para acceder al sistema, cuando realmente se está utilizando para registrar todas sus actividades.

2.5.2.2 SISTEMA DE DETECCIÓN DE INTRUSOS PARA RED (NIDS)

Monitoriza los paquetes que circulan por la red en busca de elementos que denoten un ataque contra alguno de los sistemas. Puede situarse en cualquiera de los hosts o en un elemento que analice todo el tráfico, entre estos:

- Campos de fragmentación IP.
- Dirección origen y destino
- Puerto origen y destino
- Flags TCP
- Campo de datos

2.5.2.3 DETECCIÓN DE ANOMALÍAS

El principio de funcionamiento de estos sistemas es de admitir que una anomalía en el sistema puede representar una intrusión. Se basa en la comparación de eventos suscitados en función de un conjunto de patrones almacenados y actualizados. Se puede utilizar métodos estadísticos y especificaciones de reglas que determinan los perfiles de comportamiento normal del sistema.

2.5.2.4 DETECCIÓN DE USOS INDEBIDOS

Este tipo de IDS funciona en base del establecimiento de patrones de los diferentes ataques que existen. De esta manera conociendo lo que es normal y permitido en una red, todo lo diferente a esto será detectado como una intrusión. Para ello se utiliza:

- Sistemas expertos.
- Transición de estados.
- Comparación y emparejamiento de patrones.
- Detección basada en modelos.

2.5.3 DMZ

Una zona desmilitarizada (DMZ, demilitarized zone) o red perimetral es una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet. El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones desde la DMZ sólo se permitan a la red externa →los equipos (hosts) en la DMZ no pueden conectar con la red interna. Esto permite que los equipos (hosts) de la DMZ puedan dar servicios a la red externa a la vez que protegen la red interna en el caso de que intrusos comprometan la seguridad de los equipos (host) situados en la zona desmilitarizada. Para cualquiera de la red externa que quiera conectarse ilegalmente a la red interna, la zona desmilitarizada se convierte en un callejón sin salida (Guijarro, 2012). Esta zona evita grandes riesgos a los que se ve expuesta una red ya que trabaja conjuntamente con un firewall. En la **FIGURA 2. 9** se muestra su diagrama.

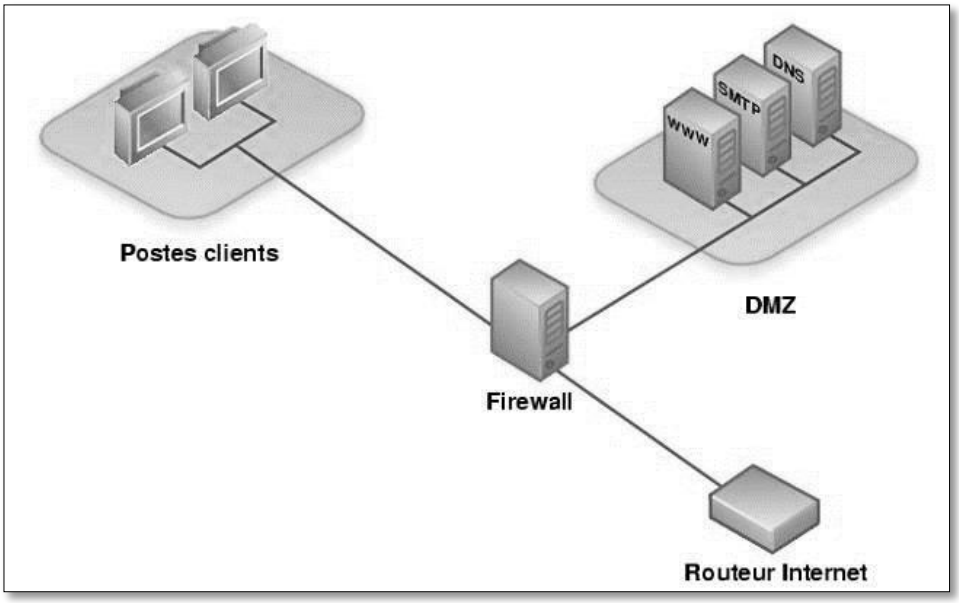


FIGURA 2. 9: Zona DMZ

Fuente: http://www.pymesyautonomos.com/tecnologia/zona-dmz-la-red-a-salvo-de-curiosos-en-la-empresa

2.5.4 POLÍTICAS DE SEGURIDAD

Las políticas de seguridad recogen las directrices u objetivos de una empresa u organización con respecto a la seguridad de la información. Forma parte de su política general y, por lo tanto, ha de ser aprobada por la dirección o consejo directivo.

El objetivo principal al redactar políticas de seguridad es de concienciar a todo el personal de la organización, particularmente a los involucrados directos con el sistema de información, en la necesidad de conocer los principios que rigen la seguridad en la entidad y cuáles son las normas para conseguir los objetivos planificados. Por tal motivo, las políticas deberán redactarse de forma clara y concisa para que sea comprendida por todo el personal de la organización.

No todas las políticas de seguridad son las mismas. El contenido depende de la realidad y requerimientos de cada organización para la que se elabora.

Las políticas de seguridad se basan en los objetivos de la empresa en cuestión englobados en los principales aspectos.

- Identificar las necesidades de seguridad y los riesgos que amenazan al sistema de información, así como evaluar los impactos ante un eventual ataque.
- Relacionar todas las medidas de seguridad que deben implementarse para afrontar los riesgos de cada activo o grupos de activos de la organización.
- Proporcionar una perspectiva general de las reglas y los procedimientos que deben aplicarse para afrontar los riesgos identificados en los diferentes departamentos de la organización.
- Detectar todas las vulnerabilidades del sistema de información y controlar los fallos que se producen en los activos, incluidas las aplicaciones instaladas.
- Definir un plan de contingencias.

2.6 NORMATIVAS

En la actualidad existen varios estándares que garantizan la protección de los Sistemas Informáticos así como un buen uso de la información. Contar con uno de ellos garantiza que la tecnología de la información dispondrá de un valor agregado en seguridad.

2.6.1 ISO/IEC 27002:2013

La Serie ISO/IEC 27000 fue publicada en el año 2000 y traducida al español en 2006; es un conjunto de estándares no certificables que proporcionan un marco de gestión de la Seguridad de Información, aplicable a cualquier tipo de organización, es dirigida a los responsables de iniciar, implantar o mantener la seguridad de una organización.

Esta norma establece directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización. Los objetivos indicados en esta norma brindan una guía general sobre las metas aceptadas comúnmente para la gestión de la seguridad de la información. (NTE INEN-ISO/IEC 27002:2013)

2.6.1.1 ESTRUCTURA DE LA NORMA

“Esta norma contiene 14 secciones sobre controles de la seguridad que en conjunto tienen un total de 35 categorías principales de la seguridad” (NTE INEN-ISO/IEC 27002:2013).

2.6.1.2 CLÁUSULAS

“Cada cláusula contiene una cantidad de categorías principales de la seguridad. Estas 14 cláusulas (acompañadas por la cantidad de categorías principales de la seguridad incluida en cada numeral) son:” (NTE INEN-ISO/IEC 27002:2013).

- Políticas de seguridad.
- Aspectos organizativos de la seguridad de la información
- Seguridad ligada a los recursos humanos
- Gestión de activos.
- Control de accesos.
- Cifrado
- Seguridad física y Ambiental
- Seguridad en la operativa
- Seguridad en las telecomunicaciones
- Adquisición, desarrollo y mantenimiento de los sistemas de información.
- Relaciones con suministradores.
- Gestión de incidentes en la seguridad de la información.
- Aspectos de seguridad de la información en la gestión de la continuidad del negocio.
- Cumplimiento

Estos catorce dominios se dividen en 35 objetivos de control y 114 controles que representan las prácticas, procedimientos o mecanismos para reducir el nivel de riesgo y se detallan a continuación [ISO/IEC 27002:2013]

2.6.1.2.1 POLÍTICAS DE SEGURIDAD

Su objetivo es dirigir y dar soporte a la gestión de la seguridad de la información; debe ser redactada, documentada, aprobada y concientizada de tal manera que sea clara y comprensible para todos los usuarios.

Cuenta con un objetivo de control y dos controles los que se muestran a continuación en la **FIGURA 2. 10**

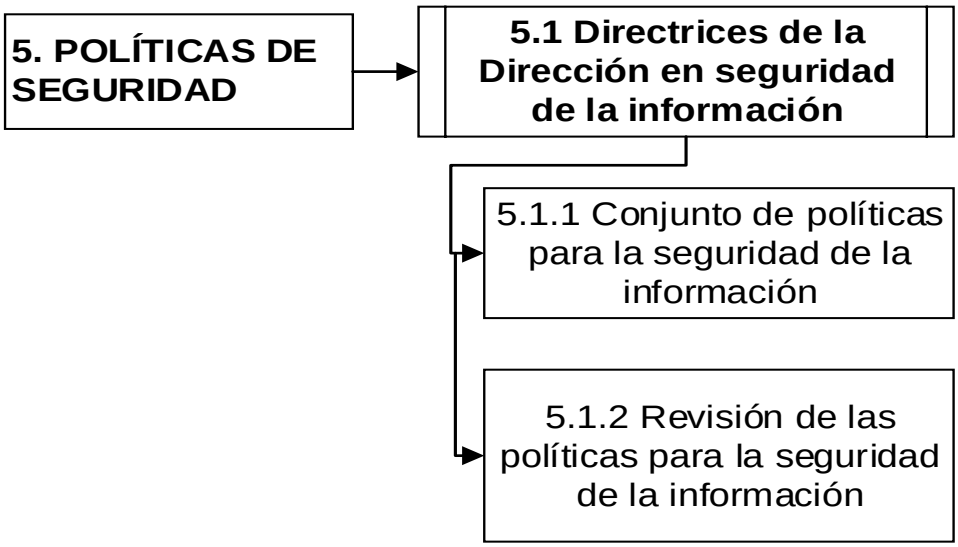


FIGURA 2. 10: Esquema del 1er dominio de la Norma ISO/IEC 27002:2013
Fuente: Adaptada de NTE INEN ISO/IEC 27002

2.6.1.2.2 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

Aquí se establece una estructura organizativa estableciendo las responsabilidades que tiene cada usuario o área de trabajo relacionada con la seguridad de los sistemas de información. Cuenta con dos objetivos de control y siete controles en total, los que se muestran a continuación en la **FIGURA 2. 11**

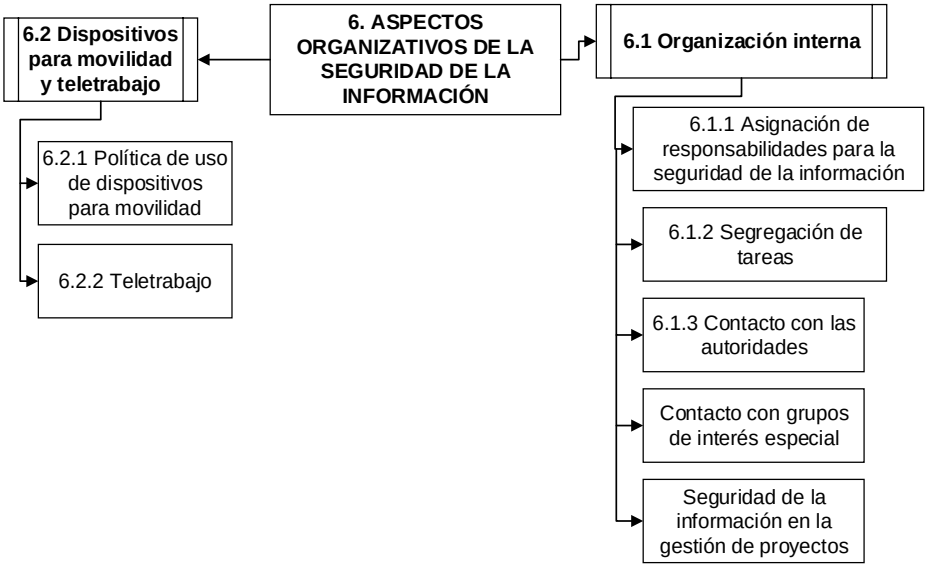


FIGURA 2. 11: Esquema del 2do dominio de la Norma ISO/IEC 27002:2013

Fuente: Adaptada de NTE INEN ISO/IEC 27002

2.6.1.2.3 SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

Se trata de concienciar a los empleados de la empresa sobre los riesgos que pueden ocasionar al operar incorrectamente los sistemas de información o cualquier componente de este. Esto se lleva a cabo mediante la evaluación y asignación de responsabilidades de seguridad. Cuenta con tres objetivos de control y seis controles en total, los que se muestran a continuación en la **FIGURA 2. 12**

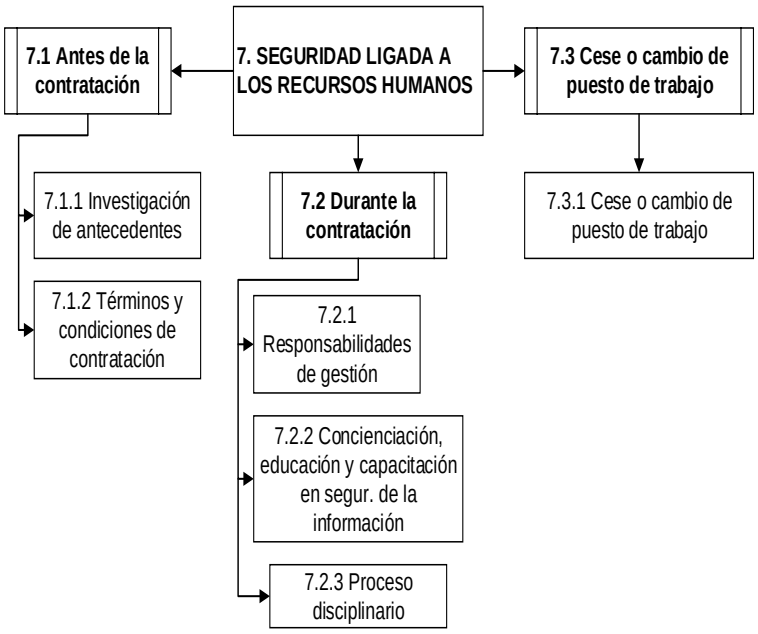


FIGURA 2. 12: Esquema del 3er dominio de la Norma ISO/IEC 27002:2013

Fuente: Adaptada de NTE INEN ISO/IEC 27002

2.6.1.2.4 GESTIÓN DE ACTIVOS

Su finalidad es proteger adecuadamente los activos de la organización, clasificándolos, manteniendo un inventario actualizado, y proporcionando a cada uno el nivel de protección que le corresponde.

Cuenta con tres objetivos de control y diez controles en total, los que se muestran en la **FIGURA 2. 13**

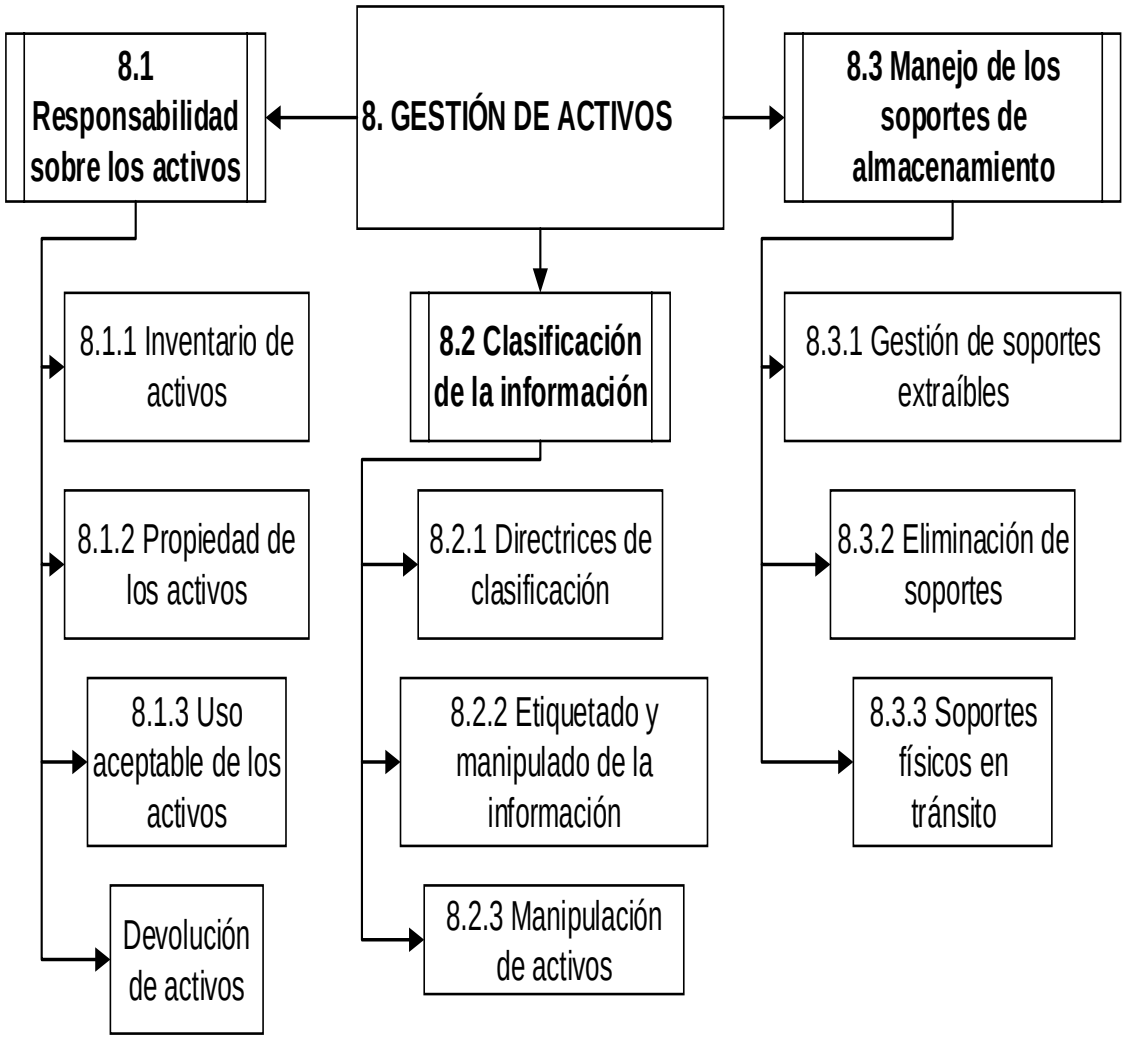


FIGURA 2. 13: Esquema del 4to dominio de la Norma ISO/IEC 27002:2013.
Fuente: Adaptada de NTE INEN ISO/IEC 27002

2.6.1.2.5 CONTROL DE ACCESOS

Su objetivo es evitar accesos no autorizados a la información, equipos y servicios de la organización. Está compuesto de cuatro objetivos de control y catorce controles en total, los que se muestran a continuación en la **FIGURA 2. 14:** Esquema del 5to dominio de la Norma ISO/IEC 27002:2013

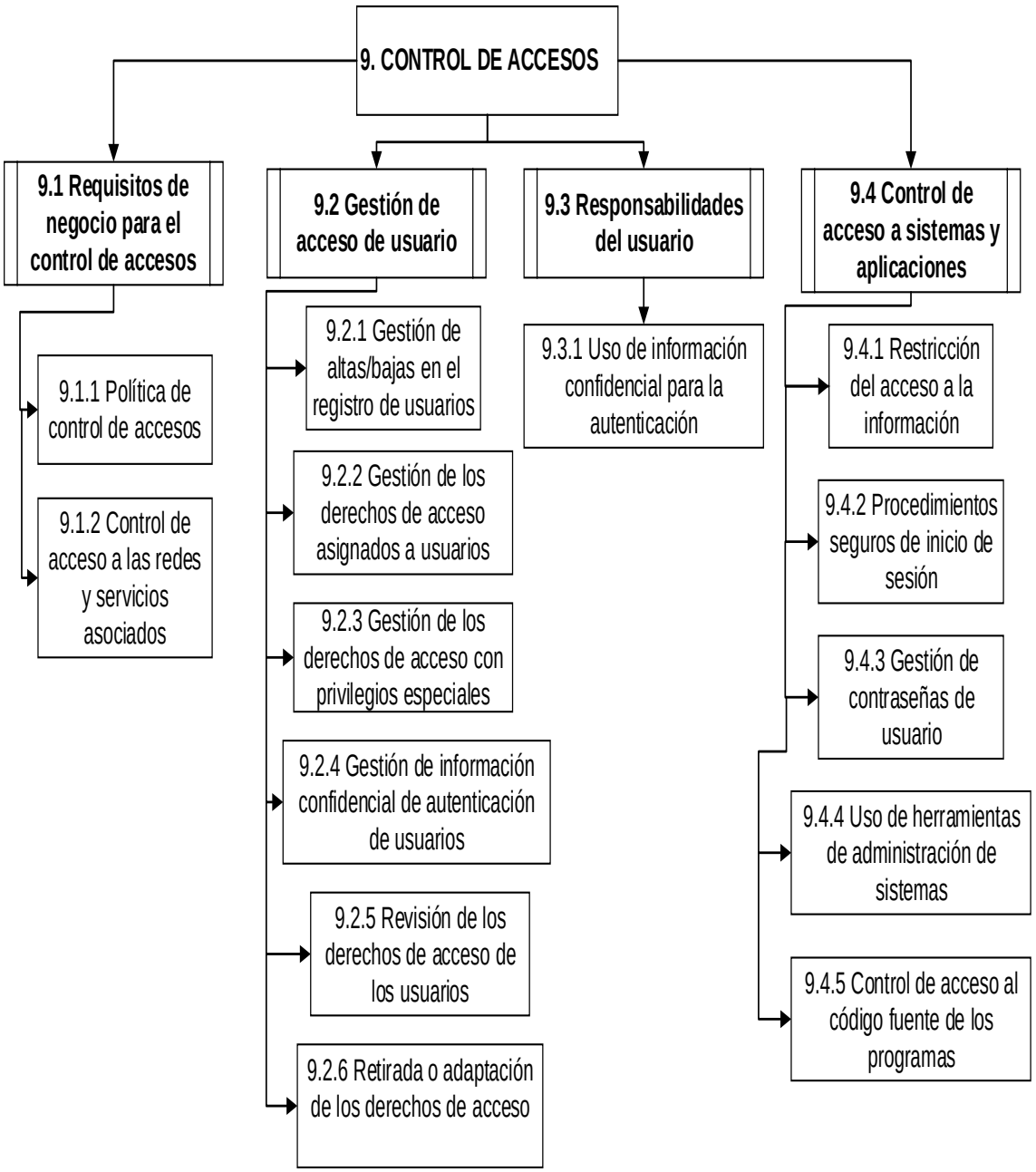


FIGURA 2. 14: Esquema del 5to dominio de la Norma ISO/IEC 27002:2013

Fuente: Adaptada de NTE INEN ISO/IEC 27002

2.6.1.2.6 CIFRADO

Su objetivo es establecer controles criptográficos y manejar adecuadamente las claves de acceso a los diferentes aplicativos del sistema de información. Está compuesto de un objetivo de control y dos controles en total, los que se muestran a continuación en la **FIGURA 2. 15**

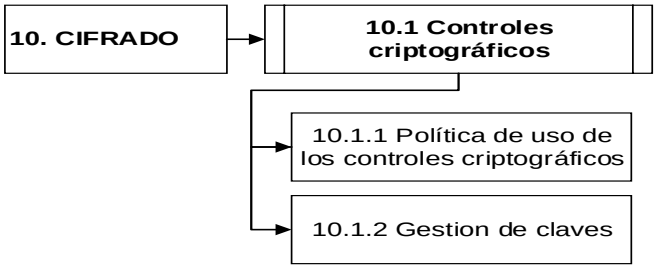
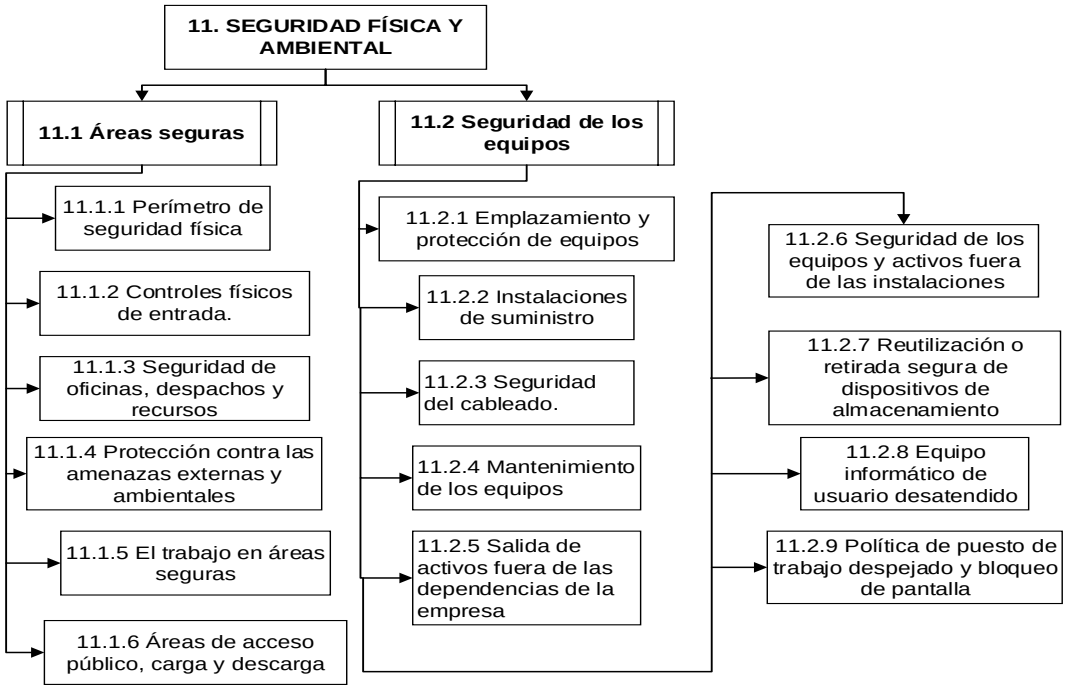


FIGURA 2. 15: Esquema del 6to dominio de la Norma ISO/IEC 27002:2013

Fuente: Adaptada de NTE INEN ISO/IEC 27002

2.6.1.2.7 SEGURIDAD FÍSICA Y AMBIENTAL

Su objetivo es delimitar y controlar el acceso a las diferentes áreas de trabajo, así como también dar protección contra amenazas externas y ambientales. Cuenta con dos objetivos de control y quince controles en total, los que se muestran en la **FIGURA 2. 16**



.

FIGURA 2. 16: Esquema del 7mo dominio de la Norma ISO/IEC 27002:2013

Fuente: Adaptada de NTE INEN ISO/IEC 27002

2.6.1.2.8 SEGURIDAD EN LA OPERATIVA

Garantiza la correcta operación de la información para lo cual se establece procedimientos para proteger los documentos, medios informáticos, datos de entrada o salida y documentación del sistema, de daño, modificación, robo y acceso no autorizado.

Cuenta con siete objetivos de control y catorce controles en total, los que se muestran en la **FIGURA 2. 17**

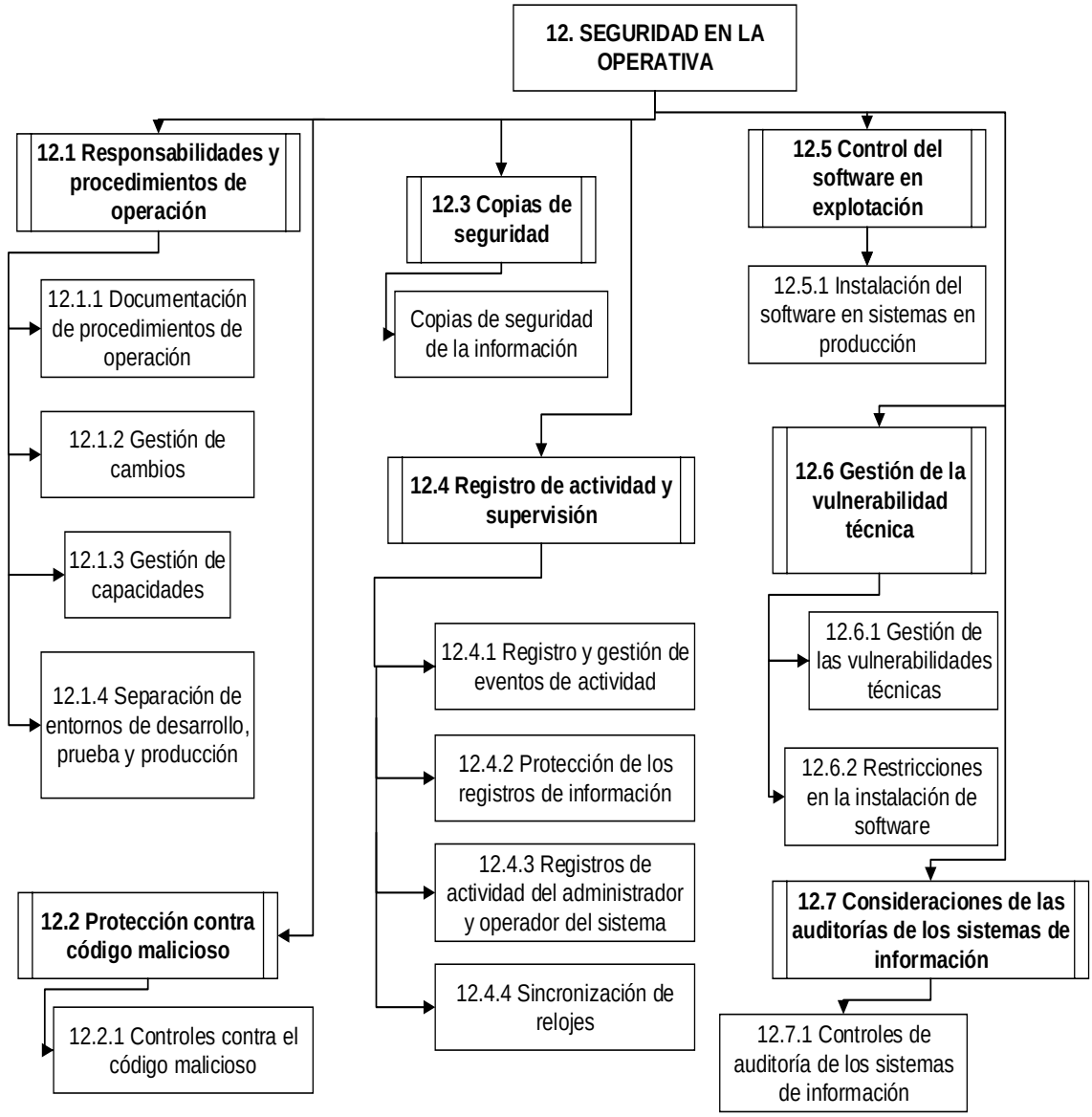


FIGURA 2. 17: Esquema del 8vo dominio de la Norma ISO/IEC 27002:2013

Fuente: Adaptada de NTE INEN ISO/IEC 27002

2.6.1.2.9 SEGURIDAD EN LAS TELECOMUNICACIONES

Su función es mantener la integridad y disponibilidad de los servicios de información y telecomunicación, protegiendo la información en las redes y su infraestructura de apoyo. Cuenta con dos objetivos de control y siete controles en total, los que se muestran en la **FIGURA 2. 18**

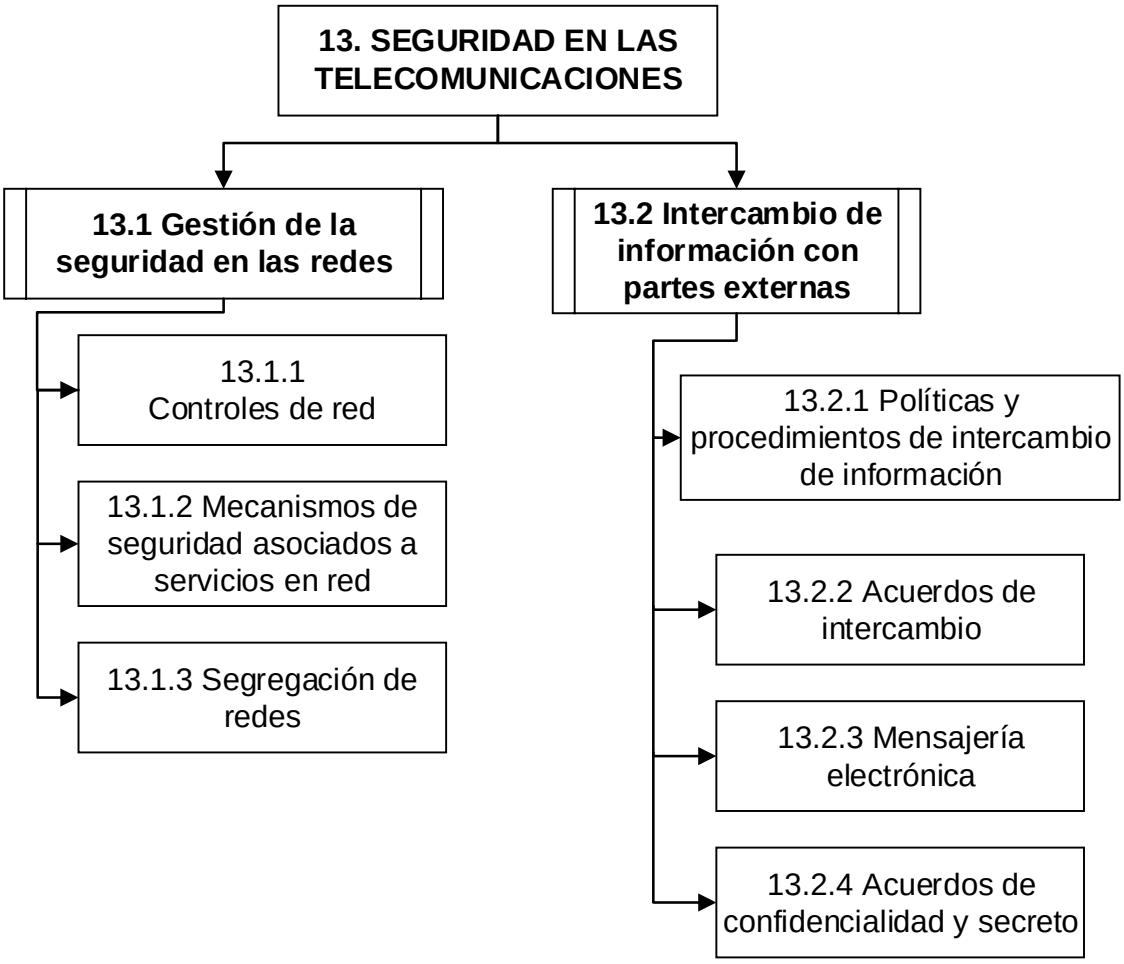


FIGURA 2. 18: Esquema del 9no dominio de la Norma ISO/IEC 27002:2013

Fuente: Adaptada de NTE INEN ISO/IEC 27002

2.6.1.2.10 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

Su principal objetivo es la administración de la seguridad en el desarrollo, mantenimiento y operación exitosa del sistema de información, evitando pérdidas, modificaciones o mal uso de los datos de usuario en las aplicaciones. Dispone de tres objetivos de control y trece controles en total, los que se muestran en la **FIGURA 2. 19**

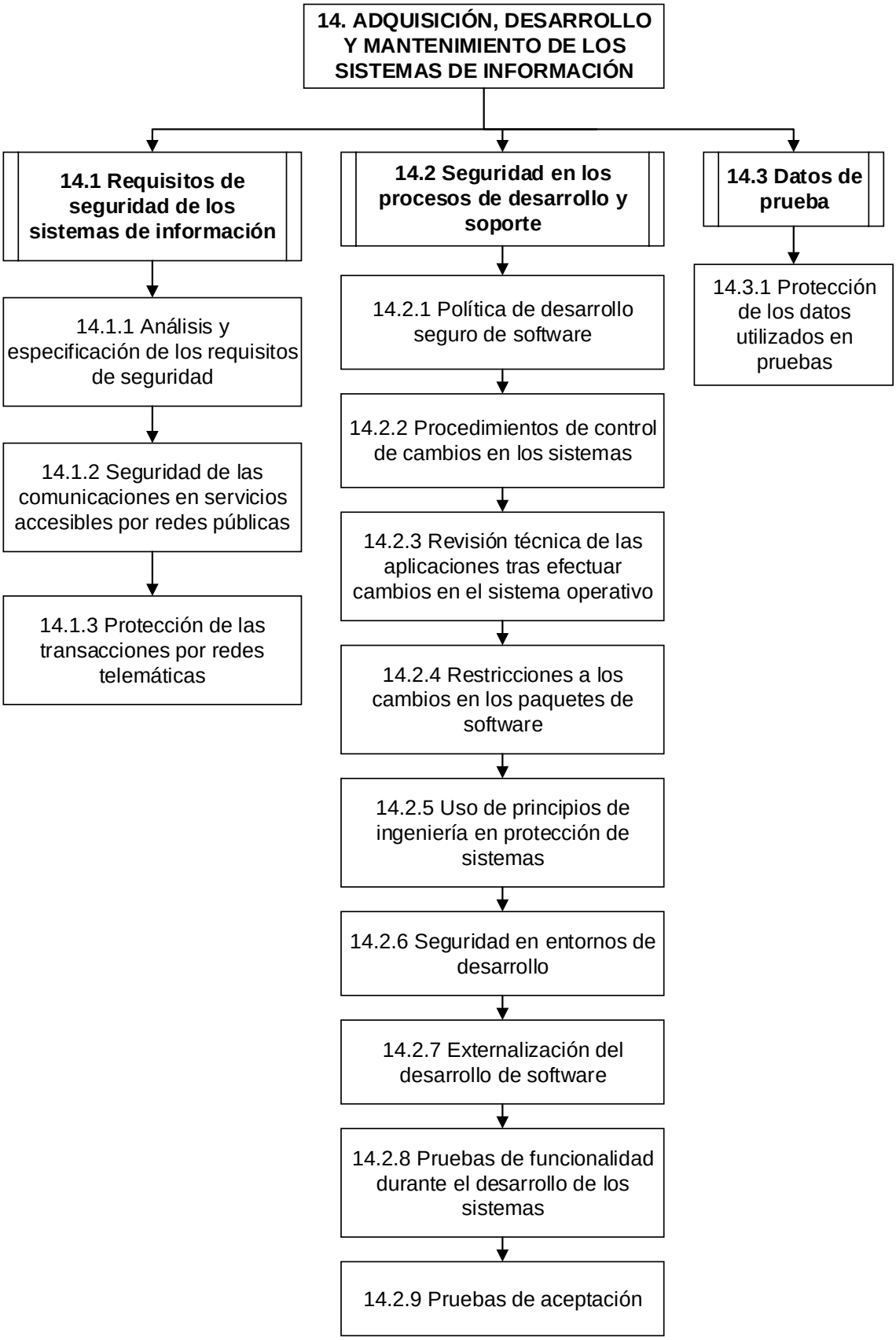


FIGURA 2. 19: Esquema del 10mo dominio de la Norma ISO/IEC 27002:2013

Fuente: Adaptada de NTE INEN ISO/IEC 27002

2.6.1.2.11 RELACIONES CON SUMINISTRADORES

Su fin es documentar los requisitos de seguridad de la información para contrarrestar los riesgos a los que se ve expuesta la organización al permitir el acceso de proveedores a los activos. Dispone de dos objetivos de control y cinco controles en total, los que se muestran en la **FIGURA 2. 20**

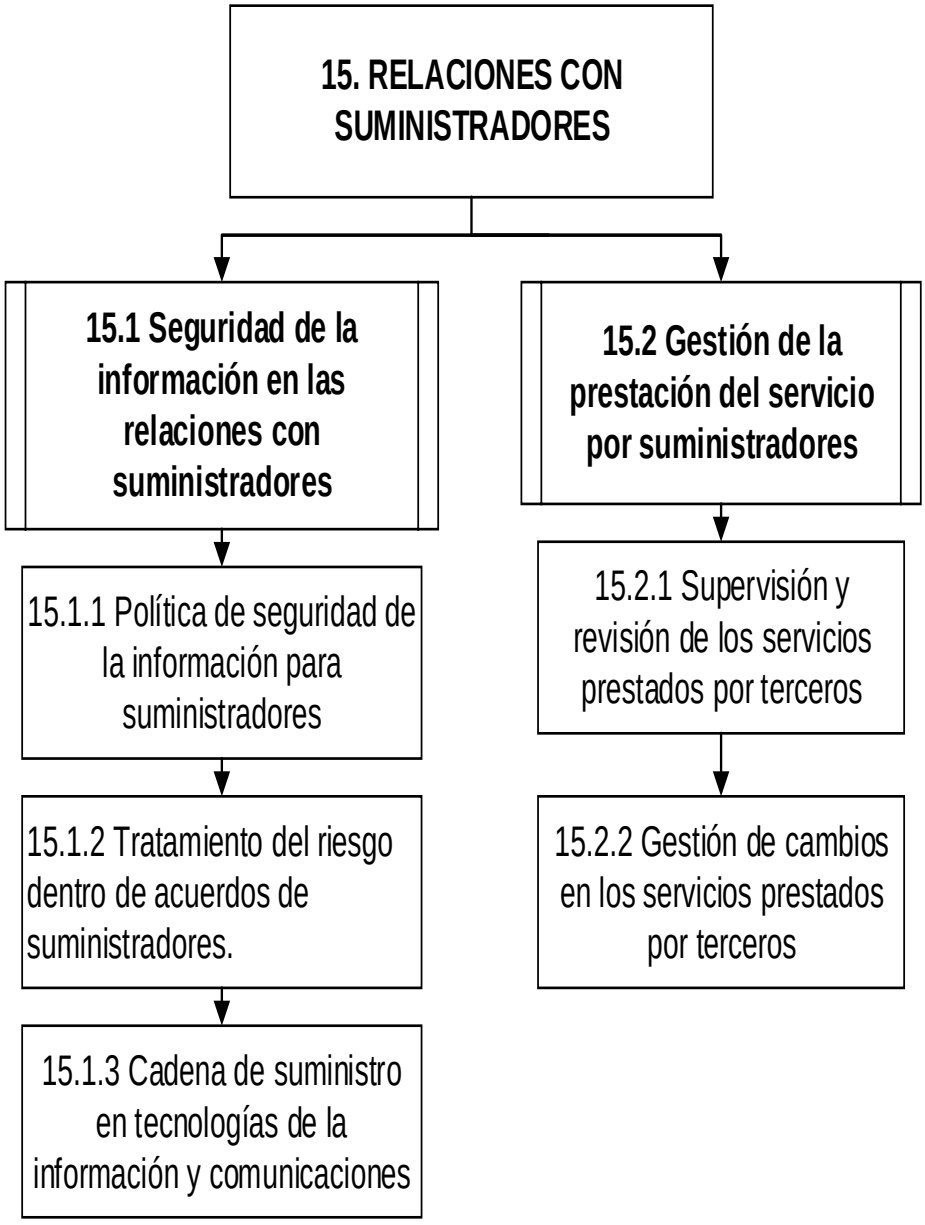


FIGURA 2. 20: Esquema del 11vo dominio de la Norma ISO/IEC 27002:2013

Fuente: Adaptada de NTE INEN ISO/IEC 27002

2.6.1.2.12 GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN

Asigna responsabilidades y procedimientos de gestión que notifiquen un evento inapropiado que genere riesgo a la seguridad de la información, reuniendo la evidencia necesaria para la adecuada toma de decisiones.

Dispone de un objetivo de control y siete controles, los que se muestran en la **FIGURA 2. 21**

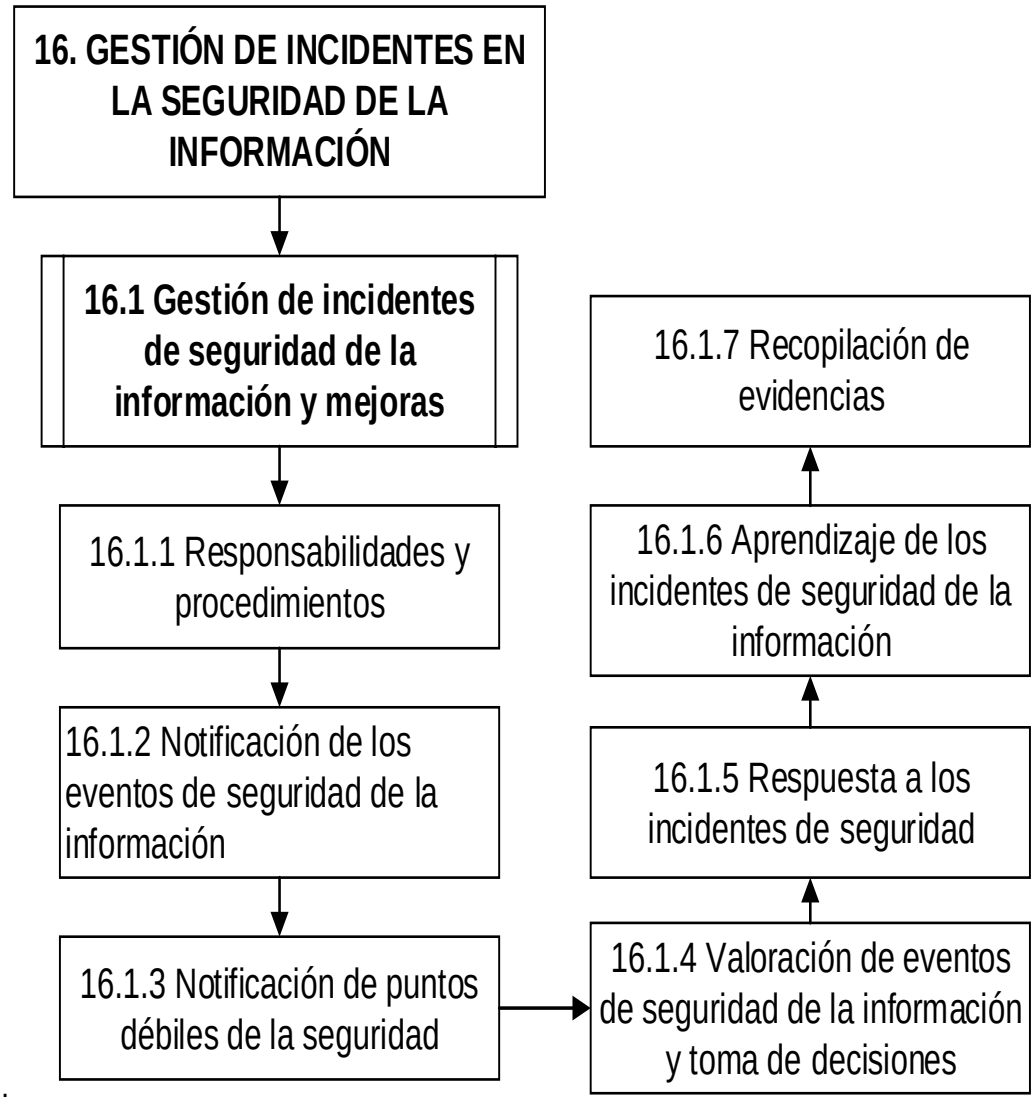


FIGURA 2. 21: Esquema del 12vo dominio de la Norma ISO/IEC 27002:2013

Fuente: Adaptada de NTE INEN ISO/IEC 27002

2.6.1.2.13 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

El objetivo es reaccionar inmediatamente ante interrupciones causadas por las actividades del negocio o desastres naturales, evitando la perdida de información y dinero.

Dispone de dos objetivos de control y cuatro controles en total, los que se muestran en la **FIGURA 2. 22**

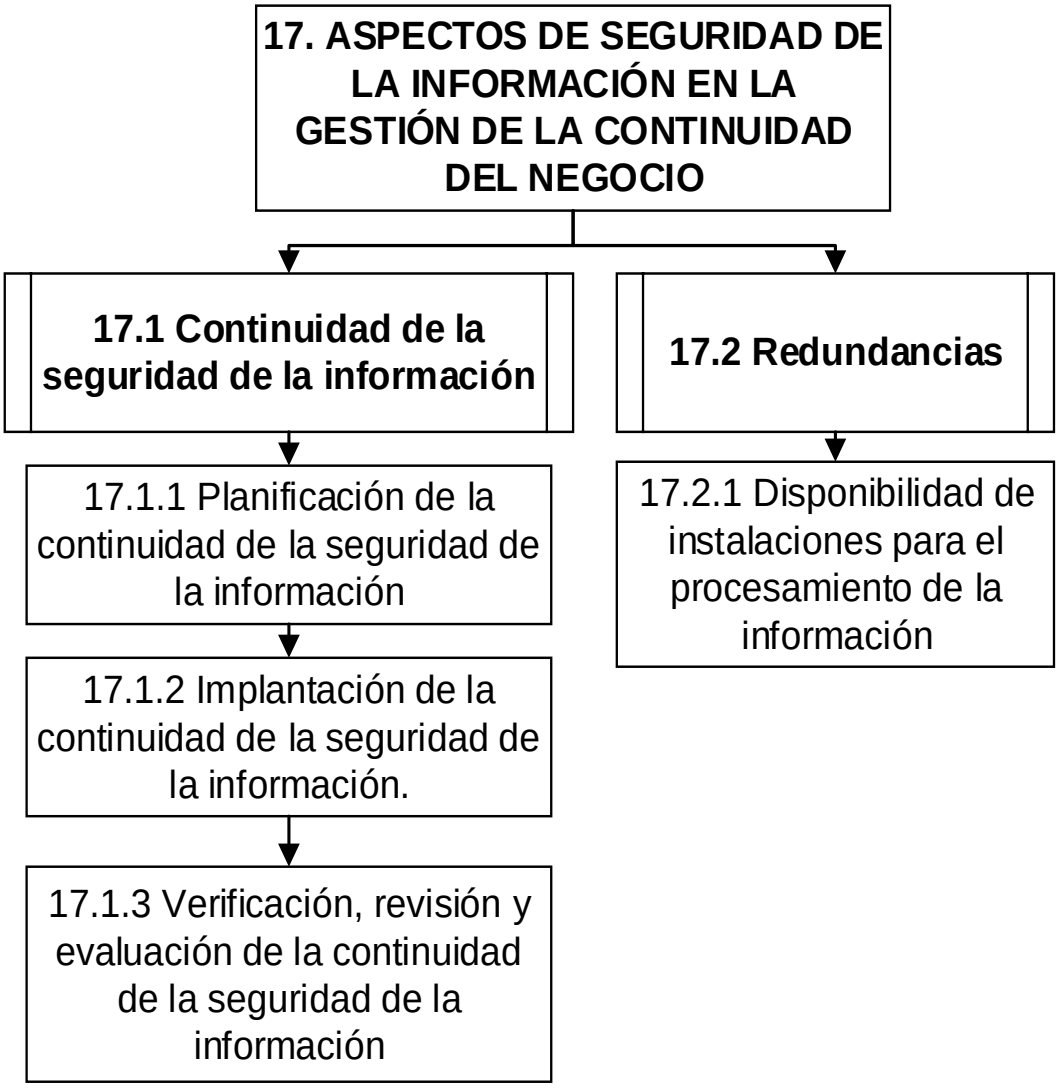
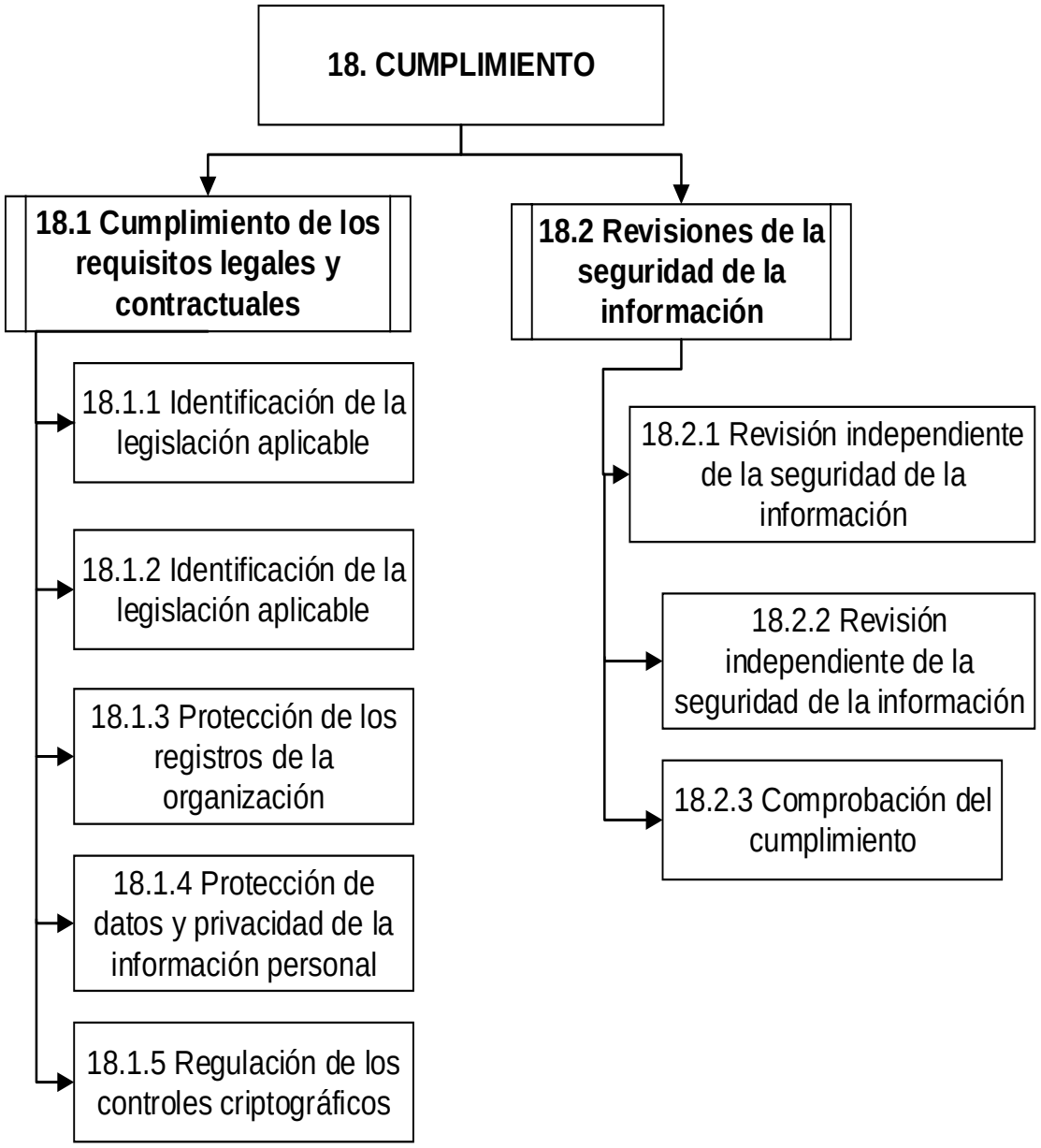


FIGURA 2. 22: Esquema del 13vo dominio de la Norma ISO/IEC 27002:2013

Fuente: Adaptada de NTE INEN ISO/IEC 27002

2.6.1.2.14 CUMPLIMIENTO

Se encarga de evitar el incumplimiento de cualquier ley, estatuto, regulación y de cualquier requisito de seguridad de la organización. Dispone de dos objetivos de control y ocho controles en total, mismos que se muestran en la **FIGURA 2. 23**



.

FIGURA 2. 23: Esquema del 14vo dominio de la Norma ISO/IEC 27002:2013

Fuente: Adaptada de NTE INEN ISO/IEC 27002

2.7 INTRODUCCIÓN AL ANÁLISIS DE RIESGOS

En la actualidad existen diferentes metodologías para el análisis de riesgos de la seguridad de la información de una entidad pública o privada. En vista de que en la ISO/IEC 27002:2013 no se especifica ninguna metodología; para este estudio se seleccionó la metodología OSSTMM (Manual de la metodología abierta de testeo de seguridad) la misma que se describirá a lo largo de esta sección.

2.7.1 OSSTMM

OSSTMM es un manual de metodologías para pruebas y análisis de seguridad. El manual se encuentra realizado por ISECOM (Institute for Security and Open Methodologies). Es una organización dirigida por Pete Herzog, dedicada al desarrollo de metodologías de libre utilización para la verificación de la seguridad, programación segura, verificación de software y concientización en seguridad.

- Este manual contempla el cumplimiento de normas y mejores prácticas como la ISO/IEC 27002; siendo así el complemento para la realización de este trabajo.
- Expresa con un valor numérico el nivel de seguridad de una organización.
- Provee guías para el auditor de sistemas, destinadas a la certificación de la organización en cuanto a los requisitos del ISECOM

Permite obtener un test certificado de OSSTMM; el mismo que sirve como prueba de un testeo de OSSTMM minucioso, además brinda una apropiada visión general, dándole al cliente una declaración precisa sobre el testeo.

2.7.1.1 PROPÓSITO

El principal objetivo es proveer una metodología científica para examinar la organización, realizando pruebas de la seguridad de adentro hacia afuera. Otro objetivo es proporcionar guías para el auditor de sistemas, destinadas a la certificación de la organización en cuanto a los requisitos del ISECOM.

El Documento provee una serie de descripciones específicas para el desarrollo de un test de seguridad operacional sobre todos los canales incluyendo aspectos físicos, humanos, telecomunicaciones, medios inalámbricos, redes de datos y cualquier otra descripción de una métrica real (Valdez Alvarado, 2013).

2.7.1.2 AMBITO

El ámbito debe abarcar toda la seguridad operativa, y comprometerse en las diferentes áreas o canales como lo describe el manual, y se observa en la **FIGURA 2. 24**

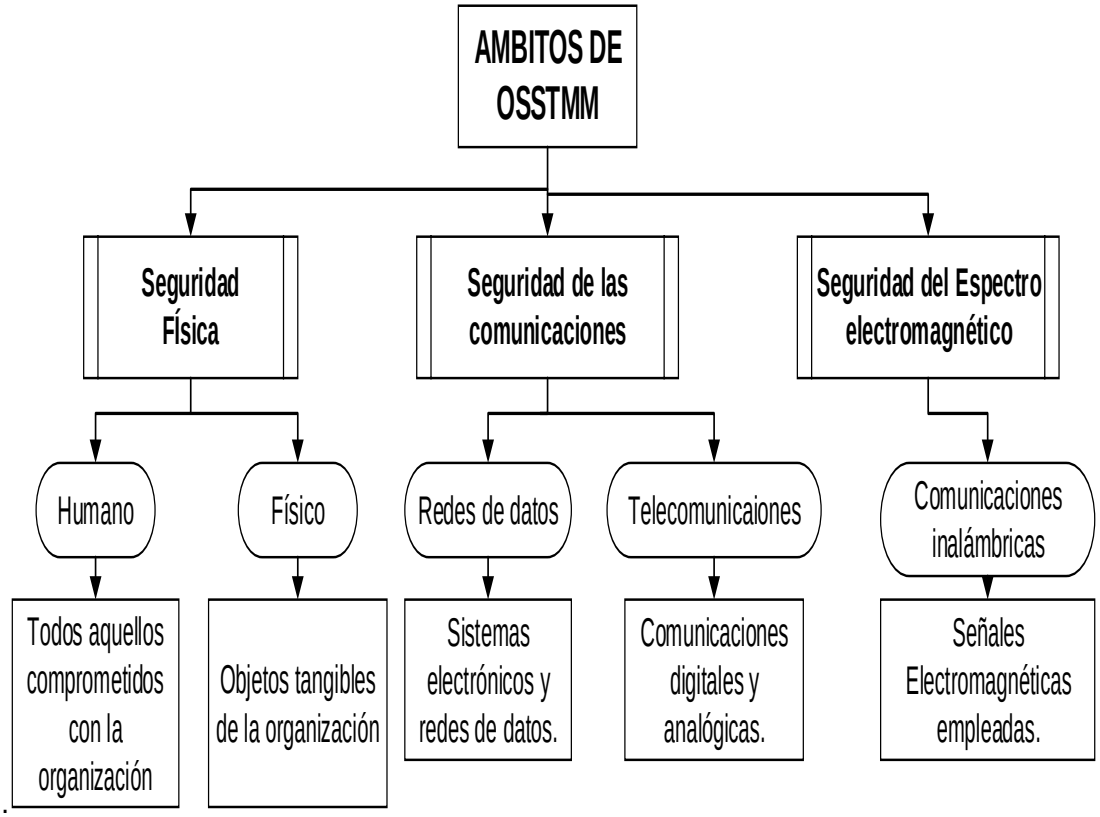


FIGURA 2. 24: Ámbitos de OSSTMM

Fuente: (Valdez Alvarado, 2013)

2.7.1.3 FASES

OSSTMM está conformada por cuatro fases:

2.7.1.3.1 FASE DE REGLAMENTACIÓN

Cada viaje comienza con una dirección. En la fase de regulación, el auditor comienza la auditoría con una comprensión de los requisitos de auditoría, el alcance y las limitaciones a la auditoría de este alcance. A menudo, el tipo de prueba se determina mejor después de esta fase (Herzog, OSSTMM 3.0, 2003).

2.7.1.3.2 FASE DE DEFINICIÓN

"El centro del test seguridad básica requiere conocer el alcance en relación a las interacciones con los objetivos transmitidos a las interacciones con los activos. En esta fase se definirán los aspectos" (Herzog, OSSTMM 3.0, 2003).

2.7.1.3.3 FASE DE INFORMACIÓN

El auditor va descubriendo información, donde la intención es descubrir la mala gestión de la información. En esta fase se considera la verificación de procesos, de configuración, la validación de propiedad, una revisión de segregación y de exposición, una exploración de la Inteligencia Competitiva (Valdez Alvarado, 2013).

2.7.1.3.4 FASE INTERACTIVA DE PRUEBAS DE CONTROLES

Estas se centran en la penetración y perturbación. Es por lo regular la fase final de las pruebas de seguridad, y esta no puede realizarse mientras las otras no se hayan realizado. En esta fase se considera la verificación de la cuarentena, la auditoria de privilegios, la validación de sobrevivencia, revisión de alertas y registros (Valdez Alvarado, 2013).

2.7.1.4 PROCESO

El proceso de un análisis de seguridad, se concentra en evaluar los ítems de la estructura presentada en OSSTMM 3.0, basados en el cálculo del RAV[3].

2.7.1.4.1 PROCESO DE CUATRO PUNTOS

El proceso de los cuatro puntos son las instrucciones específicas y los medios utilizados para llegar a los informes; asegurando de esta manera una revisión integral. Los cuatro puntos que intervienen en dicho proceso se muestran y explican en la **TABLA 2. 1**

[3] El RAV es una medición de la escala de la superficie de ataque, la cantidad de interacciones no controladas con un objetivo, que se calcula por el equilibrio cuantitativo entre las operaciones, limitaciones y controles. (Herzog, OSSTMM 3.0, 2003)

TABLA 2. 1: Proceso de 4 puntos OSSTMM.

PROCESO DE 4 PUNTOS			
Fases	**Descripción**	**Etapas**	**Descripción**
Inducción	Estudiar el entorno donde reside el objetivo.	Revisión del entorno	Conocer las normas, leyes, políticas y cultura organizacional que influyen en los requerimientos de seguridad.
		Logística	Obtener detalles del canal de análisis para evitar falsos positivos o falsos negativos.
		Verificación de detección activa	Averiguar si existen controles que detecten intrusiones que puedan filtrar o bloquear intentos de análisis.
		Auditoría de visibilidad	Enumerar los objetivos visibles dentro del alcance.
Interacción	Interactuar directamente con el objetivo y observar las respuestas obtenidas	Verificación de accesos	Determinar los puntos de acceso, la forma de interacción y el propósito de su existencia.
		Verificación de confianza	Verificar las relaciones de confianza entre los objetivos, donde exista acceso a la información sin necesidad de autenticación.
		Verificación de controles	Verificar la efectividad de controles de proceso
Fases	**Descripción**	**Etapas**	**Descripción**
		Verificación de procesos.	Comprobar el mantenimiento y efectividad de los niveles de seguridad en los procesos establecidos.

		Verificación de la configuración.	Revisar el funcionamiento de los procesos en condiciones normales.
		Validación de propiedad.	Revisar la procedencia de los datos, información, sistemas, etc.
		Revisión de segregación	Revisar los controles que aseguran separación entre la información personal y organizacional.
Investigación	Analizar los indicadores que provengan del objetivo.	Verificación de exposición.	Buscar información, disponible de manera abierta, que permita conocer detalles del objetivo.
		Exploración de inteligencia de negocios.	Verificar la existencia de fuentes de información que contengan datos de negocio que debieran ser confidenciales
Intervención	Modificar los recursos del entorno que necesita el objetivo y observar cómo responde.	Verificación de cuarentena.	Verificar la efectiva separación de elementos hostiles.
		Auditoría de privilegios.	Analizar el correcto uso de los sistemas de autenticación y autorización.
		Continuidad de negocio.	Analizar la efectividad de los controles de resistencia y continuidad.
		Alerta y revisión de logs.	Verificar si la relación entre las actividades realizadas y los registros almacenados es correcta.

Fuente: Adaptada de (Herzog, OSSTMM 3.0, 2003).

2.7.1.4.2 DIAGRAMA DE FLUJO

“Juntando los módulos que derivan del proceso de cuatro puntos se obtiene un diagrama de flujo que define una metodología aplicable a cualquier tipo de test y sobre cualquier canal” (Toth & Sznek, 2014). El mismo que se muestra en la **FIGURA 2. 25**

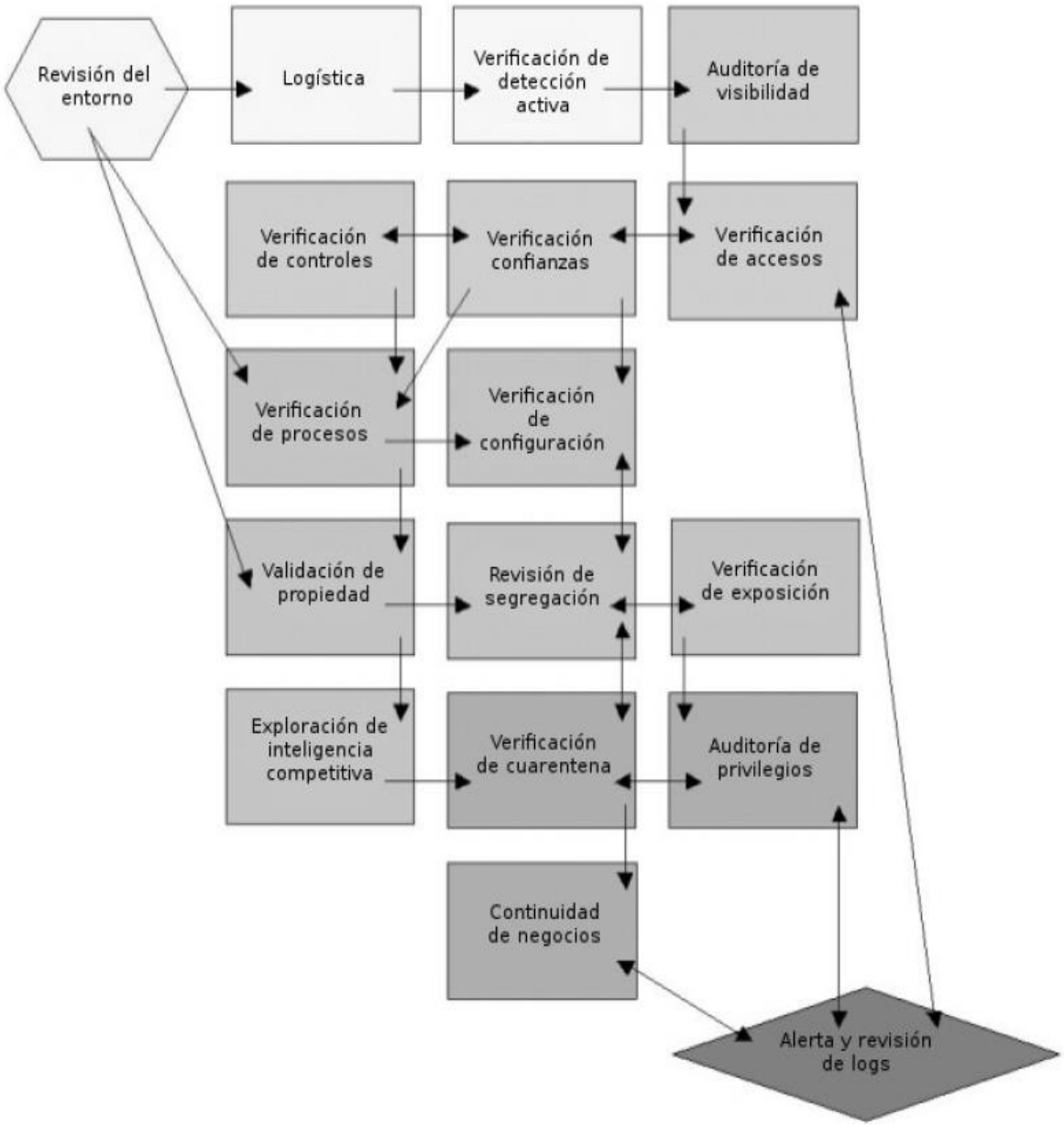


FIGURA 2. 25: Diagrama de flujo OSSTMM

Fuente: Tomada de (Toth & Sznek, 2014)

El diagrama anterior permite obtener los datos requeridos como entrada para determinar la seguridad de la información en un momento determinado.

2.7.1.5 SEGURIDAD OPERACIONAL

El primer paso será calcular el RAV en la seguridad operacional, la misma que se define como “la medida de la visibilidad, accesos y confianza dentro del alcance.” (Toth & Sznek, 2014)

2.7.1.5.1 VISIBILIDAD

“Componentes de la presencia de seguridad que pueden ser remotamente identificados” (Herzog, OSSTMM 2.1, 2003).

Por ejemplo para realizar una auditoría, en la sección “Humana” se emplea a 60 personas; sin embargo, sólo 45 de ellos son interactivos a partir del vector de prueba y canal. Esto haría una visibilidad de 45. (Herzog, OSSTMM 3.0, 2003)

2.7.1.5.2 ACCESOS

El acceso es el punto de entrada al nivel de seguridad. Un punto de acceso no requiere ser una barrera física. Esto puede incluir, pero no se limita a, una página web, una ventana, una conexión de red, ondas de radio, o cualquier cosa cuya ubicación soporte la definición de casi-público o donde un computador interactúa con otro por medio de una red (Herzog, OSSTMM 2.1, 2003).

Por ejemplo en una auditoría física, si se tiene un edificio con 2 puertas y 12 ventanas abiertas se trata de un Acceso de 14. Si se sierran todas las puertas y ventanas, a continuación, se trata de una Acceso de 0 ya que estos no son los puntos donde se puede obtener la entrada (Herzog, OSSTMM 3.0, 2003).

2.7.1.5.3 CONFIANZA

“La confianza es una ruta especializada en relación con el nivel de seguridad. La confianza incluye la clase y cantidad de autenticación, no-repudio, control de acceso, contabilización, confidencialidad e integridad entre dos o más factores dentro del nivel de seguridad.” (Herzog, OSSTMM 2.1, 2003)

“Por ejemplo, un proxy que redirige todo el tráfico de entrada a un equipo que procesa la petición sin verificar el origen, representaría una confianza” (Toth & Sznek, 2014)

1.7.1.6 CONTROLES

Definir los controles es un paso muy importante y necesario para el cálculo del RAV ya que constituyen mecanismos de seguridad y protección durante interacciones.

2.7.1.6.1 AUTENTICACIÓN

“La autenticación es la medida por la cual cada interacción en el proceso está privilegiada” (Toth & Sznek, 2014)

Por ejemplo en una auditoría en la Sección Física, si se requiere tanto una tarjeta de identificación especial y un biométrico para acceder, a continuación, se puede añadir 2 para la autenticación. Sin embargo, si el acceso sólo requiere uno o el otro, entonces sólo se cuenta 1 a la autenticación. (Herzog, OSSTMM 3.0, 2003)

2.7.1.6.2 INDEMNIZACIÓN

Es un compromiso entre el propietario del activo y la parte que interactúa. Puede ser un aviso legal para el caso en que una de las partes no cumpla con las reglas prefijadas; o puede ser un seguro contratado a terceros para el caso que se produzcan fallas o pérdidas de algún tipo (Toth & Sznek, 2014).

Por ejemplo en un seguro de bienes, que tiene como alcance 200 computadoras, una póliza de seguro contra él se aplica a todas los 200 y por lo tanto se una cuenta de 200 (Herzog, OSSTMM 3.0, 2003).

2.7.1.6.3 SUBYUGACIÓN

“Define las condiciones en las cuales ocurrirán las interacciones. Esto quita libertad en la forma de interacción pero disminuye los riesgos” (Toth & Sznek, 2014)

Por ejemplo en una auditoria de sección Humana, Toth & Sznek recalcan en un proceso de no repudio donde la persona debe firmar un registro y proporcionar un número de identificación para recibir un documento se encuentra bajo controles de subyugación cuando el proveedor del documento registra el número de identificación, en lugar de que lo haga el receptor para eliminar el registro de un número falso con un nombre falso.

2.7.1.6.4 CONTINUIDAD

“Permite mantener la interacción con los activos aun en caso de fallas” (Toth & Sznek, 2014)

Por ejemplo en una auditoría física, si se descubre que una puerta de entrada a una tienda se bloquea de forma que no hay alternativa de entrada y los clientes no pueden entrar, entonces este acceso no tiene continuidad. (Herzog, OSSTMM 3.0, 2003)

2.7.1.6.5 RESISTENCIA

"Es el mecanismo que brinda protección a los activos en caso que las interacciones sufran alguna falla" (Toth & Sznek, 2014)

Por ejemplo en una auditoría de Sección Física el control de 2 guardias de acceso a una puerta, si uno se retira y la puerta no se puede abrir por el guardia restante, entonces tiene la capacidad de resistencia.

2.7.1.6.6 NO REPUDIO

Herzog en el Manual de OSSTMM 2.1 define el no repudio como aquel que, "provee garantía que ninguna persona o sistema responsable de la interacción pueda negar envolvimiento en la misma."

2.7.1.6.7 CONFIDENCIALIDAD

Herzog, (OSSTMM 2.1) Señala que la confidencialidad, "es la certeza que únicamente los sistemas o partes involucradas en la comunicación de un proceso tengan acceso a la información privilegiada del mismo."

"Un ejemplo claro de confidencialidad es la encriptación" (Herzog, OSSTMM 3.0, 2003)

2.7.1.6.8 PRIVACIDAD

Herzog, Señala que la privacidad, "implica que el proceso es conocido únicamente por los sistemas o partes involucradas."

Un ejemplo claro puede ser "simplemente tomando la interacción en un cuarto cerrado lejos de otras personas" (Herzog, OSSTMM 3.0, 2003)

2.7.1.6.9 INTEGRIDAD

"Permite identificar cuando un activo ha sido modificado por alguien ajeno a la interacción en curso" (Toth & Sznek, 2014)

"En una auditoria en las redes de datos, el cifrado puede proporcionar el control de la integridad sobre el cambio del archivo en la transmisión" (Herzog, OSSTMM 3.0, 2003)

2.7.1.6.10 ALARMA

“Es la notificación apropiada y precisa de las actividades que violan o intentan violar cualquiera de las dimensiones de la seguridad. En la mayoría de violaciones de seguridad, la alarma es el único proceso que genera reacción” (Herzog, OSSTMM 2.1, 2003)

“En una auditoria en las redes de datos, se cuenta cada servidor y el servicio que brinda: cuenta como una alarma al ser monitoreado por el sistema de detección de intrusos” (Herzog, OSSTMM 3.0, 2003)

2.7.1.6.11 LIMITACIONES

“Las limitaciones son aquellos inconvenientes que se presentan en los controles, con el objetivo de separar los activos y las amenazas” (Toth & Sznek, 2014)

2.7.1.6.12 VULNERABILIDAD

“Es una falla que puede permitir el acceso no autorizado a un activo o puede denegar dicho acceso a alguien que si este autorizado.

2.7.1.6.13 DEBILIDAD

“Es una falla que reduce o anula los efectos de los controles de interacción”.

2.7.1.6.14 PREOCUPACIÓN

“Es una falla que reduce los efectos de los controles de proceso.”

2.7.1.6.15 EXPOSICIÓN

“Es una acción injustificada que permite dejar visible, ya sea de forma directa o indirecta, a un activo.”

2.7.1.6.16 ANOMALÍA

“Es un elemento desconocido y no se encuentra dentro de las operaciones normales. Por lo general es síntoma de algún fallo pero que todavía no se comprende.”

CAPÍTULO III

3 SITUACIÓN ACTUAL Y ANÁLISIS DE RIESGOS

En este capítulo se dará a conocer como está formada la red, que equipos dispone, los riegos a los que se ven expuestos y su impacto frente al desempeño de la empresa. Se realizará también el análisis de los riesgos mediante la aplicación de la metodología OSSTMM.

3.1 SITUACIÓN ACTUAL

Comprende en describir el estado actual de su infraestructura de red, equipos y servicios en lo referente a la seguridad de los mismos.

3.1.1 HISTORIA DE LA EMPRESA

“Somos una Cooperativa de Ahorro y Crédito con 6 años de vida institucional, siendo considerada entre las más exitosas y representativas de la Colectividad Ecuatoriana, hecho que nos ha permitido congregar una gran familia más de 10,000 asociados ESCENCIA INDÍGENA fue creada por un grupo de jóvenes Indígenas visionarios, emprendedores de la provincia de Tungurahua e Imbabura, fue entonces que esta sociedad comenzó con reuniones semanales, como no se contaban con suficiente recursos para emprender grandes proyectos, se empezó con aportes económicos mensuales con lo cual se reunió un capital, iniciándose el otorgamiento de préstamos a corto plazo y especialmente para los miembros del grupo. Para aquella época se habían constituido en una asociación de comerciantes informales.

En el 2006 surgieron muchas ideas orientadas a cómo ayudar al desarrollo de las personas de escasos recursos económicos no solo del grupo ni de la comunidad sino de toda la Provincia, entonces nació la Cooperativa de Ahorro y Crédito "Escencia Indígena" con el acuerdo ministerial 0000111 el 16 de noviembre de 2006 emitida en la ciudad de Quito por las autoridades de la Dirección Nacional de Cooperativas, también con un objetivo de rescatar la interculturalidad de los pueblos indígenas Mestizas y Afro Ecuatorianas del Ecuador La propuesta de constituir una Cooperativa de Ahorro y Crédito con oficinas ubicadas en la ciudad de Ibarra en la calle Juana Atabalipa 2-46 y Rafael Larrea (Parque Germán Grijalva) Fue entonces que el 19 de mayo del 2007 se abre las puertas en la ciudadanía de Ibarra y posteriormente nos expandimos en el Ecuador”.

3.1.2 CRECIMIENTO PROYECTADO

El crecimiento de la red de la Cooperativa de Ahorro y crédito Escencia Indígena Ltda ha sido progresivo de acuerdo a las necesidades económicas de los sectores que rodean a esta empresa de tipo financiero.

En la actualidad la cooperativa cuenta con 10 agencias ubicadas a nivel nacional las mismas que se encuentran interconectadas y forman parte de la red de la cooperativa Escencia Indígena; en la **FIGURA 3. 1** se detalla su ubicación geográfica.

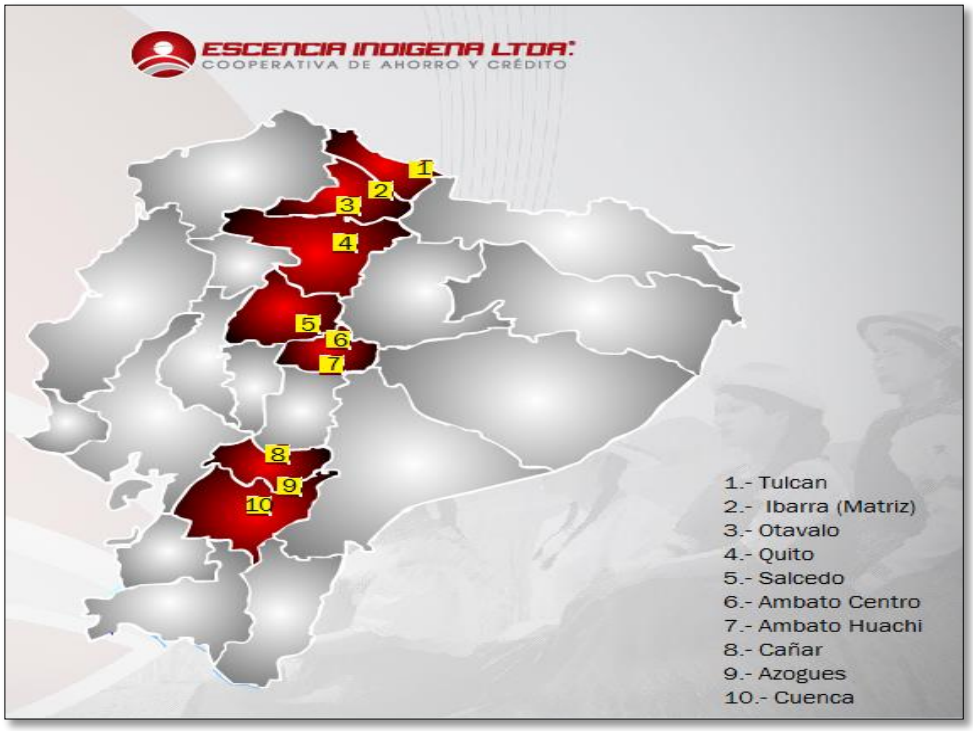


FIGURA 3. 1: Ubicación Geográfica de las sucursales.

Fuente: Editada de http://www.escenciaindigena.com/cobertura/

3.1.3 POLÍTICAS DE OPERACIÓN

La cooperativa cuenta con ciertas políticas relacionadas a las acciones y responsabilidades de los trabajadores dentro de la empresa más no cuenta con un manual sobre políticas y buenas prácticas de seguridad de la información y de los activos de la empresa.

3.1.4 PROCEDIMIENTOS ADMINISTRATIVOS

Aquí se muestra la como se encuentra organizada la empresa.

3.1.4.1 ORGANIGRAMA INSTITUCIONAL

Se asignan las funciones de los diferentes cargos administrativos para un mejor desempeño y administración de la empresa, como se ve en la **FIGURA 3. 2**

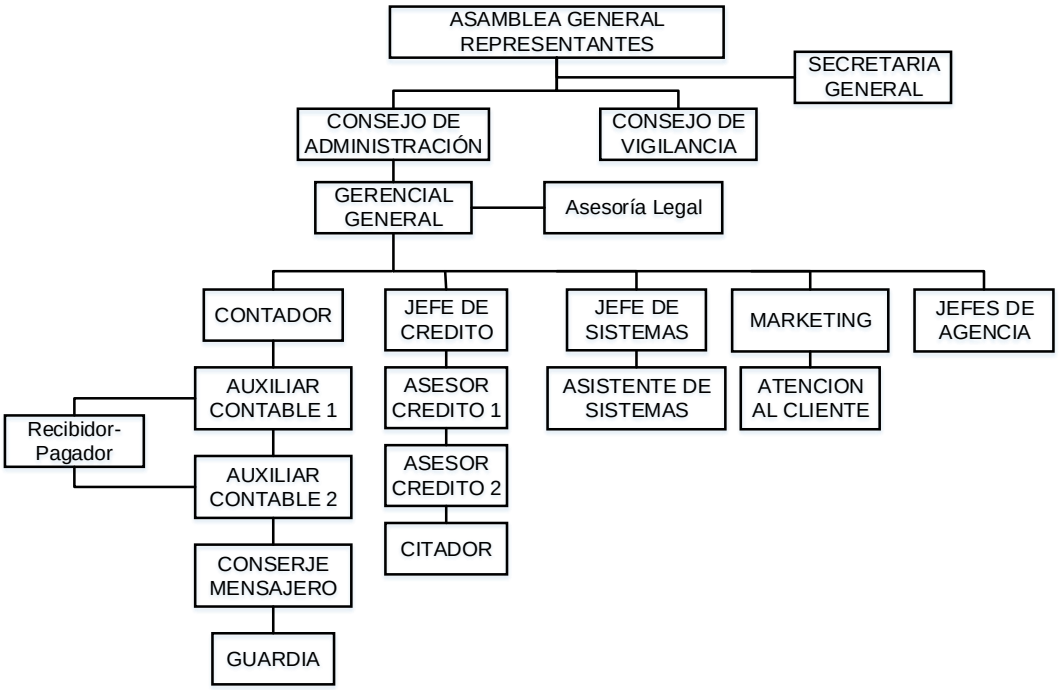


FIGURA 3. 2: Organigrama institucional

Fuente: COAC Escencia Indígena

3.2 SERVICIOS Y PRODUCTOS

Entre los principales productos que ofrece se encuentran: cuentas de ahorro, créditos, depósito a plazo fijo, cajeros automáticos, pago del bono de desarrollo humano, pago del bono de desnutrición cero, crédito de desarrollo humano, pago de servicios básicos, transferencias internacionales, sistema nacional de pagos, pago SOAT latina seguros.

3.3 ACTIVOS TECNOLÓGICOS DE LA EMPRESA

A continuación se nombran los activos de mayor importancia para el correcto desempeño de las funciones de la cooperativa.

3.3.1 CENTRO DE PROCESAMIENTO DE DATOS (DATA CENTER)

Actualmente la cooperativa Escencia Indígena no cuenta con un centro de procesamiento de datos totalmente calificado, únicamente dispone de un espacio en el tercer piso en el cual se albergan los equipos servidores de aplicaciones y de servicio.

El acceso a este lugar no cuenta con sistema robusto de control de acceso, únicamente se dispone de una chapa. El ambiente no es el adecuado ya que este sirve también de bodega de archivos y dispositivos en desuso.

3.3.2 SERVIDOR DE APLICACIONES JBOSS

Este servidor provee el servicio de correo electrónico y la página web de la empresa. En el servicio de correo institucional se tiene configurado para que el acceso al mismo sea a través de un usuario y contraseña misma que por seguridad debe ser cambiada cada 15 días.

El dominio de la página web es http://www.escenciaindigena.com por medio de la cual la ciudadanía en general puede conocer los productos, servicios, ofertas que se ofrece. Esta página es muy interactiva con el usuario, en ella se puede conocer el estado de sus préstamos, saldos de ahorros, movimientos de cuenta y depósitos a plazo fijo mediante el servicio "Escencia en Línea", realizar cotizaciones, entre otros. A continuación se muestra la página en la **FIGURA 3. 3**

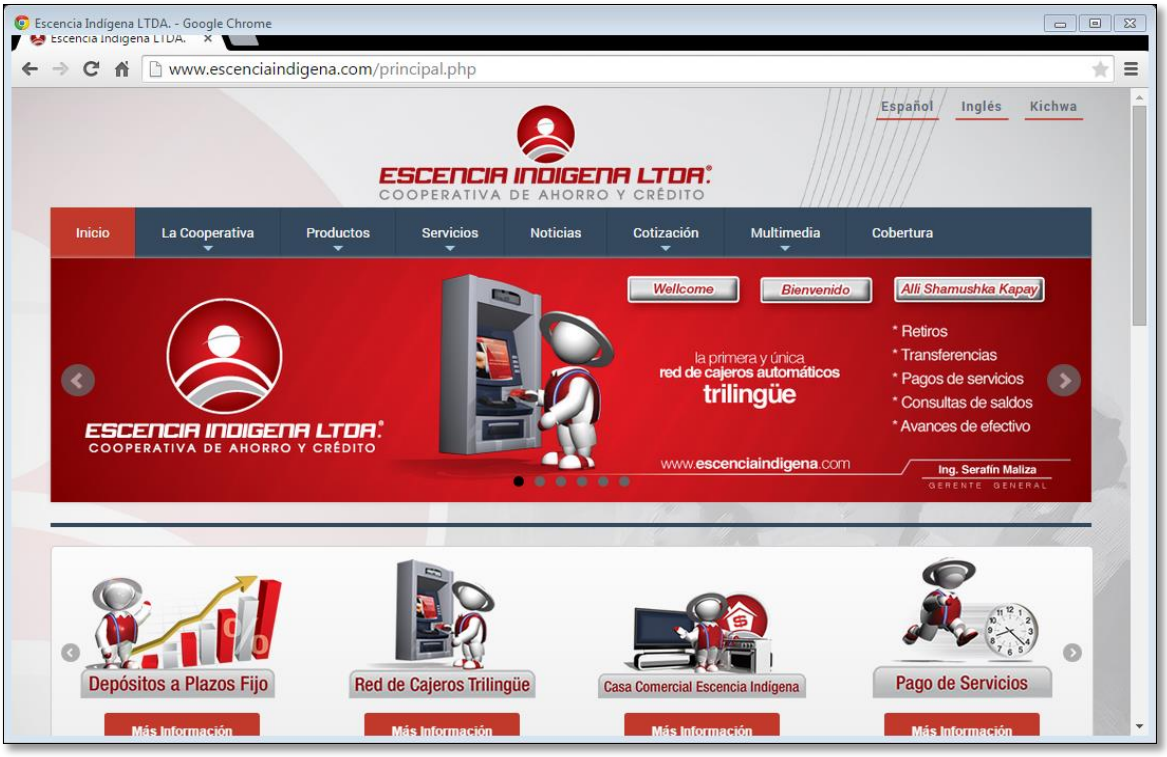


FIGURA 3. 3: Sitio Web de la institución

Fuente: http://www.escenciaindigena.com/principal.php

3.3.3 SERVIDOR PROXY

El servidor proxy controla el acceso de los usuarios a internet y a los servidores en especial al de base de datos. El flujo es permitido o denegado en base a las reglas establecidas como medida de seguridad.

3.3.4 ROUTER CNT (CORPORACIÓN NACIONAL DE TELECOMUNICACIONES)

El proveedor de servicio de internet en la matriz de la cooperativa Escencia indígena es la Corporación Nacional de Telecomunicaciones el cual ha instalado un router ubicado en el cuarto de equipos cuyo enlace físico es mediante fibra óptica de última milla.

3.3.5 CABLEADO ESTRUCTURADO

El cableado estructurado ha sido implementado con cable UTP categoría 6A de cuatro pares cumpliendo con las características eléctricas, físicas y mecánicas de acuerdo a la norma TIA/EIA 568-B.

El cableado horizontal del punto más lejano de red no sobrepasa los 90 metros. El resto de elementos como jacks, faceplaces, patch panels, conectores Rj-45 son compatibles con la categoría 6A del cable UTP.

3.3.6 SISTEMA DE AIRE ACONDICIONADO

Las instalaciones de la cooperativa no cuenta con un sistema propiamente dicho de acondicionamiento que incluya sensores de temperatura, salvo el caso del cuarto de equipos que si dispone de un equipo de aire acondicionado marca LG; en las demás oficinas se cuenta con ventiladores convencionales.

3.3.7 SISTEMA DE ALIMENTACIÓN ININTERRUMPIDA (UPS)

En el caso de interrupción de la energía eléctrica, el cuarto de equipos cuenta con un equipo UPS de 8000VA y 6400 watts encargado de brindar soporte de energía a los dispositivos de red, servidores y otros sistemas electrónicos de la cooperativa.

3.3.8 CONTROL DE ACCESO

El cuarto de equipos, espacio físico de mayor importancia y el que mayor cuidados debe tener no cuenta con un sistema robusto de control de acceso. El ingreso está totalmente libre exponiendo los servidores a manipulaciones indebidas.

3.3.9 CÁMARAS DE SEGURIDAD

Como parte del sistema de seguridad la cooperativa cuenta con 6 cámaras de seguridad las cuales están ubicadas en los diferentes ambientes de la organización. Los videos se almacenan por dos semanas, pasado este tiempo se borran automáticamente situación que no es muy conveniente ya que se debería realizar una copia de seguridad antes de ser borrados definitivamente para aclarar cualquier imprevisto que pudiese presentarse.

3.3.10 SISTEMA DE CONTROL DE DETECCIÓN Y EXTINCIÓN DE INCENDIOS

Como parte de la detección de incendios se cuenta con sensores detectores de humo, además como requerimiento obligatorio se dispone de los extintores uno en cada área o espacio de trabajo, los empleados se encuentran capacitados para reaccionar a la brevedad posible en caso de presentarse un incendio.

3.3.11 INTERNET

Internet es un servicio disponible para todos los funcionarios de la empresa como herramienta primordial en el desarrollo de sus actividades. Este se lo asigna manualmente mediante Ips Estáticas y no por DHCP para un mejor control de los usuarios conectados a la red; este servicio es proporcionado por el ISP de la Corporación nacional de telecomunicaciones CNT-Ep.

3.4 DETERMINACIÓN DEL RIESGOS EN LA RED DE DATOS DE LA COOPERATIVA SIGUIENDO LA METODOLOGÍA DE OSSTMM

OSSTMM 3.0 especifica una metodología de análisis de riesgos utilizando métricas operacionales de seguridad; las mismas que permiten la realización de una prueba de seguridad con mediciones exactas sobre el estado de la seguridad. Es así que con la ayuda de dichas métricas se cran los RAV, que no son más que una descripción imparcial y objetiva de una superficie de ataque.

3.4.1 SEGURIDAD FÍSICA

En el área de seguridad física interviene el medio humano y físico, en los cuales se evalúan los diferentes módulos de los 4 puntos de interacción que involucran al proceso de OSSTMM.

3.4.1.1 CANAL HUMANO

“El objetivo de realizar pruebas de seguridad en este canal es verificar la concienciación sobre la seguridad personal y medir la responsabilidad con el estándar de seguridad requerido, incluye políticas de la empresa, regulaciones de la industria, o la legislación regional” (Herzog, OSSTMM 3.0, 2003). Los resultados obtenidos se presentan a continuación.

3.4.1.1.1 SEGURIDAD OPERACIONAL

Seguridad Operacional, también conocida como la porosidad del alcance, es el primero de los tres factores de la seguridad real que deberían determinarse. Se mide inicialmente como la suma de la visibilidad del alcance P_V, de acceso P_A, y la confianza P_T. (Herzog, 2003)

El análisis será sobre la funcionalidad y la interacción que tiene cada funcionario de acuerdo al organigrama funcional de la cooperativa, con el departamento de sistemas y la seguridad de la información dentro de la entidad.

El resultado obtenido es:

$$P_H = P_V + P_A + P_T$$

ECUACIÓN 1: Seguridad Operacional
Fuente: Obtenida de (Herzog, OSSTMM 3.0)

$$P_H = 1+3+2$$

$$P_H = 6$$

A continuación se detalla de donde se obtuvieron los resultados de la seguridad operacional en el canal humano.

a. VISIBILIDAD

Enumerar el personal dentro del alcance tanto con acceso autorizado y no autorizado a los procesos dentro del alcance, sin importar la hora o el canal de acceso, y el método para la obtención de esos datos (Herzog, 2003). En la **TABLA 3. 1** se muestran los resultados obtenidos en este canal.

TABLA 3. 1: Resultados obtenidos en el segmento Visibilidad

Resultados Segmento Visibilidad		
Metodología utilizada	Observación Directa	Encuestas
Nombres de las personas de entrada	Tarquino. M Pablo. R Wilson. P	Verónica. C Janina. S **Fabián. C (P_V)**
Tipo de Acceso	Autorizado	Restringido

Fuente: Desarrollo del proyecto

El nivel de visibilidad en el canal "Humano" será de: P_V= 1; debido a que de las tres personas que tienen restringido el acceso, una si puede acceder.

b. ACCESOS

Este es un método para evaluar los privilegios de acceso a una organización y a sus bienes a través de puntos de acceso físicos (Herzog, 2003). En la **TABLA 3. 2** se muestran los resultados obtenidos en este segmento.

TABLA 3. 2: Resultados obtenidos en el segmento accesos.

RESULTADOS SEGMENTO ACCESOS	
Metodología utilizada	Observación directa
Nombres de las personas de entrada.	Cecilia. I Elizabeth.M
Información Obtenida(P_A)	1. Aplicaciones de servidores. 2. Ubicación del cuarto de equipos. 3. Nº de extensiones Telefónicas.

Fuente: Desarrollo del proyecto

El nivel de acceso en el canal “Humano” será de: P_A = 3 debido a que se ha encontrado 3 tipos de accesos disponibles para los operarios de la empresa los mismos que se muestran en la **TABLA 3. 3**

CONFIANZA

Las pruebas de confianza al personal en el ámbito de acceso a la información o a los activos físicos de otros objetivos dentro del alcance (Herzog, 2003). Como se muestran en la **TABLA 3. 3**

TABLA 3. 3: Resultados obtenidos en el segmento Confianza

Resultados del segmento Confianza	
Metodología utilizada	Observación Directa
Nombres de las personas de entrada	Eliza C Manuel M
Tipo de Información Obtenida (P_T)	Usuarios y contraseñas a host Correos confidenciales.

Fuente: Desarrollo del proyecto

El nivel de acceso en el canal “Humano” será de: P_T = 2 ya que se consideró:

1- El acceso al equipo

2- Acceso al correo institucional.

3.4.1.1.2 CONTROLES

El siguiente paso en el cálculo de la RAV es definir los controles; los mecanismos de seguridad puestos en marcha para proteger las operaciones. En primer lugar la suma de la pérdida en los controles es LC_{Sum} debe ser determinada por la suma de las 10 categorías de las perdidas en los controles (Herzog, 2003). Tal como se muestra en la **TABLA 3. 4**

TABLA 3. 4: Lista de Controles usados en OSSTMM 3.0

Controles		
Clase A	Autenticación	LC_{Au}
	Indemnización	LC_{Id}
	Resistencia	LC_{Re}
	Subyugación	LC_{Su}
	Continuidad	LC_{Ct}
Clase B	No Repudio	LC_{NR}
	Confidencialidad	LC_{Cf}
	Privacidad	LC_{Pr}
	Integridad	LC_{It}
	Alarma	LC_{Al}

Fuente: Desarrollo del proyecto, editada de (Herzog, OSSTMM 3.0)

Así, la suma de los controles LC_{Sum} se da así:

$$LC_{Sum} = LC_{Au} + LC_{Id} + LC_{Re} + LC_{Su} + LC_{Ct} + LC_{NR} + LC_{Cf} + LC_{Pr} + LC_{Lt} + LC_{Al}$$

ECUACIÓN A.2: Suma de pérdida en los controles
Fuente: Obtenida de (Herzog, OSSTMM 3.0)

a. Autenticación

Verificar y enumerar el uso de un sistema de alerta localizada o en todo el ámbito de aplicación, registro, o un mensaje para cada pasarela de acceso a través de cada canal en el que una situación sospechosa es observada por el personal en caso de sospecha de intentos de elusión, la ingeniería social, o actividad fraudulenta. (Herzog, 2003). En la **TABLA 3. 5** se muestran los resultados obtenidos en este segmento.

TABLA 3. 5: Resultados obtenidos en el control de Autenticación

Resultados control Autenticación	
Lista de aplicaciones que necesitan autenticación.	Ingreso al sistema de inicio en los host en cada estación. Ingreso a las bases de datos. Ingreso a las aplicaciones en todos los servidores.
Bloqueo del sistema (LC_{Au})	Luego de 2 intentos.

Fuente: Desarrollo del proyecto

En este caso existen métodos adecuados de autenticación en el canal humano ya que un sistema se bloquea al segundo intento fallido. Por lo tanto: LC_{Au} =2

b. INDEMNIZACIÓN

Documentar y enumerar el abuso o la elusión de la política de los empleados, seguros, confidencialidad, no competencia, contratos de responsabilidad civil, o el uso / renuncias de los usuarios con todo el personal de acceso dentro del alcance sobre todos los canales (Herzog, 2003). En la **TABLA 3. 6** se muestran los resultados obtenidos en este control.

TABLA 3. 6: Resultados obtenidos en el control de Indemnización.

Resultados del control Indemnización	
Lista de contratos, seguros de los empleados, contratos de confidencialidad. (LC_{Id})	1. Actas entrega de equipos informáticos. 2. Actas de responsabilidad de equipos informáticos. 3. Actas de responsabilidad del buen uso de internet dentro de la entidad. 4. Acuerdo de confidencialidad de información reservada de la entidad.
Lista de abuso o elución de pollita de empleados	

Fuente: Desarrollo del proyecto

En este caso no existe abuso o elusión de la indemnización en el canal humano por parte de los empleados, pero si se tiene un control de indemnización representado por cuatro parámetros por lo tanto:

$$LC_{Id} = 4$$

c. RESISTENCIA

Enumerar y probar las insuficiencias en todos los canales del personal en el ámbito el cual la eliminación del personal de puerta de enlace permita el acceso directo a los activos (Herzog, 2003).

En la **TABLA 3. 7** se muestran los resultados obtenidos en este control.

TABLA 3. 7: Resultados obtenidos en el control de Resistencia.

Resultados Control de resistencia		
Lista del personal que interactúan en el ámbito de la seguridad de información.	Tarquino. M Fabián. C Wilson. P	
Canales	Insuficiencias	Aciertos **(LC_{Re})**
• **Físico**	X	
• **Telecomunicaciones**	X	
• **Redes de datos**	X	
• **Inalámbrico**		X

Fuente: Desarrollo del proyecto

De acuerdo al test, el control de resistencia, en todos los canales es de 1 ya que existe un acierto en el canal inalámbrico: LC_{Re} =1

d. SUBYUGACIÓN

Es un control que garantiza que las interacciones ocurran solamente de acuerdo con los procesos definidos. (Herzog, 2003)

De acuerdo al test, el control de subyugación es nulo ya que no se tiene establecido procesos estrictos; por lo cual: LC_{Su} =0

e. CONTINUIDAD

Es un control sobre todas las interacciones para mantener la interactividad con los activos en el caso de la corrupción o el fracaso.

Contar cada caso de acceso de confianza en el ámbito de aplicación lo que asegura que ninguna interrupción en la interacción a través del canal y el vector pueden ser causados, incluso en situaciones de fracaso total. La continuidad es el paraguas plazo para características como la capacidad de supervivencia, equilibrio de carga, y redundancia (Herzog, 2003). En la **TABLA 3. 8** se muestran los resultados obtenidos en este control.

TABLA 3. 8: Resultados obtenidos en el control de Continuidad

Resultados control de Continuidad	
Tipo de Test	Observación Directa
Acciones	Si el personal sale de vacaciones o por motivos de salud, o personal necesita de permiso para ausentarse ya sea por horas o días.
Observaciones (LC_{Ct})	El desarrollo de las actividades cotidianas dentro de la organización puede tener ciertas fallas, ocasionando debilidades en la continuidad.

Fuente: Desarrollo del proyecto

El control de continuidad en el canal humano es cero ya que si un empleado por cualquier motivo tiene que ausentarse de su lugar de trabajo, éste genera conflictos en el correcto desempeño de la empresa. En este caso

$$LC_{Ct} = 0$$

f. NO REPUDIO

El no-repudio provee garantía que ninguna persona o sistema responsable de la interacción pueda negar participación en la misma (Herzog, 2003).

Enumerar y probar al uso o las deficiencias del personal para identificar y registrar el acceso o la interacción con los activos de pruebas específicas para cuestionar el repudio correctamente. Documentar la profundidad de la interacción que se registra (Herzog, 2003).

De acuerdo al test, el control de No-Repudio es nulo debido a que cada empleado cuenta con un usuario el cual es registrado en toda actividad que realice por lo cual no podría negar su participación a menos que por descuido propio deje activada su cuenta y otra persona pueda acceder a ella y realizar alguna actividad; en este caso: LC_{NR} =0

g. CONFIDENCIALIDAD

"La confidencialidad es la certeza que únicamente los sistemas o partes involucradas en la comunicación de un proceso tengan acceso a la información privilegiada del mismo" (Herzog, 2003).

En esta sección, sin embargo, un método de confidencialidad puede incluir murmullo o el uso de señales manuales (Herzog, 2003). En la **TABLA 3. 9** se muestran los resultados obtenidos en este control.

TABLA 3. 9: Resultados obtenidos en el control de Confidencialidad.

Resultados control de Confidencialidad	
Tipo de Test	Murmullo
Acciones	En la COAC Escencia Indígena se realiza envío de notificaciones o peticiones mediante memorandos, u oficios, en los que se detallan información relevante para la empresa.
Observaciones (LC_{Cf})	1. Existe falta de confidencialidad debido a que ciertos documentos no son leídos únicamente por los interesados, sino también por terceras personas.

Fuente: Desarrollo del proyecto

De acuerdo al test, el control de Confidencialidad en el canal humano es 1 ya personas a las que no está destinado un oficio puede leerlo; por esta razón:

$$LC_{Cf} = 1$$

h. PRIVACIDAD

Mapa de los guardianes de los activos de información privadas dentro del ámbito de aplicación, la información que se almacena, cómo y dónde se almacena la información, y sobre las que los canales se comunica la información. En la **TABLA 3. 10** se muestran los resultados obtenidos en este control.

TABLA 3. 10: Resultados obtenidos en el control de Privacidad.

Resultados control de Privacidad	
Tipo de Test	Mapa de los guardianes de los activos de información privados.
Qué se almacena, cómo y dónde se almacena la información. (LC_{Pr})	1. Parte de la información privada se almacena en bases de datos y discos duros.

Fuente: Desarrollo del proyecto

De acuerdo al test, el control de Privacidad en el canal humano es uno ya que la información importante se almacena en la base de datos y discos duros: LC_{Pr} =1

i. INTEGRIDAD

En seguridad humana, la separación de funciones y otros mecanismos de corrupción de reducción proporcionan un control de integridad. Asegurar la integridad personal en que dos o más personas se necesitan para un único proceso para asegurar la supervisión de ese proceso. Esto incluye que no existe un maestro de acceso a todo el proceso. No puede haber una persona con acceso completo y sin llave maestra para todas las puertas. En la **TABLA 3. 11** se muestran los resultados obtenidos en este control.

TABLA 3. 11: Resultados obtenidos en el control de Integridad.

Resultados control de Integridad	
Tipo de Test	Observación directa
Lista de personas que tienen acceso a todos los lugares. (LC_{It})	1. En la cooperativa, la persona encargada de la limpieza, tiene acceso a todas las oficinas; pero no tiene acceso a lugares restringidos como el cuarto de equipos.

Fuente: Desarrollo del proyecto

De acuerdo al test, el control de Integridad es uno ya que la persona de limpieza puede acceder a todas las oficinas menos al cuarto de equipos: LC_{It} =1

j. ALARMA

Verificar y enumerar el uso de un sistema de alerta localizada o en todo el ámbito de aplicación, registro, o un mensaje para cada pasarela de acceso a través de cada canal en el que una situación sospechosa es observada por el personal en caso de sospecha de intentos de elusión, la ingeniería social, o actividad fraudulenta (Herzog, 2003).

En la **TABLA 3. 12** se muestran los resultados obtenidos en este control.

TABLA 3. 12: Resultados obtenidos en el control de Alarma.

Resultados control alarma	
Tipo de Test	Observación directa
Observaciones (LC_{Al})	1. Cuando existen alarmas emitidas por el antivirus de URLs sospechosas al acceder a ciertas páginas de internet, el usuario responde de manera adecuada a este tipo de alarmas cerrando inmediatamente la conexión.

Fuente: Desarrollo del proyecto

De acuerdo al test, el control de Alarma en el canal humano es uno por que responde adecuadamente a la notificación del antivirus al detectar un URL sospechoso: LC_{Al} =1

3.4.1.1.3 LIMITACIONES

El siguiente paso, es el cálculo de las limitaciones; las mismas que están consideradas de forma individual. La ponderación de las vulnerabilidades, debilidades y preocupaciones se basan en una relación entre la suma OpSec, la pérdida de controles.

a. VULNERABILIDAD

Contar cada defecto o error que afrontan las protecciones por el que una persona o un proceso acceden, negar el acceso a los demás, u ocultar activos dentro del alcance (Herzog, 2003).

En la **TABLA 3. 13** se muestran los resultados obtenidos en esta limitación.

TABLA 3. 13: Resultados obtenidos en la Limitación de Vulnerabilidad.

Resultados Limitación Vulnerabilidad	
Tipo de Test	Observación directa
Observaciones (L_v)	1. Debido a tendencias culturales y políticas no se da información necesaria para ocupar los nuevos puestos.

Fuente: Desarrollo del proyecto

De acuerdo al test, las vulnerabilidades son:L_v =1 por lo descrito en la tabla anterior.

b. DEBILIDAD

Es el defecto o error que interrumpe, reduce, obliga, o anula específicamente los efectos de los cinco controles de interactividad: la autenticación, la indemnización, la resistencia, la subyugación y la continuidad (Herzog, 2003). En la **TABLA 3. 14** se muestran los resultados obtenidos en esta limitación.

TABLA 3. 14: Resultados obtenidos en la limitación de Debilidad.

Resultados Limitación Debilidad	
Tipo de Test	Observación directa.
Observaciones (L_w)	1. El no haber una puerta con seguridad y control de acceso o un guardia en el acceso al cuarto de equipos.

Fuente: Desarrollo del proyecto

De acuerdo al test, el cálculo de las debilidades es:L_w =1 por la falta de seguridad en el acceso al cuarto de equipos.

c. PREOCUPACIÓN

Cuente cada defecto o error en los controles del proceso: no repudio, confidencialidad, privacidad, integridad y alarma (Herzog, 2003).

$L_C = LC_{Cf} + LC_{Al} + LC_{It} + LC_{Pr} + LC_{NR}$ → Suma de valores ya mencionados.

ECUACIÓN A.3: Cálculo de la Limitación Preocupación

Fuente: Herzog, OSSTMM 3.0

$$L_C = 1 + 1 + 1 + 1 + 0$$

$$L_C = 4$$

d. EXPOSICIÓN

Cuente cada acción injustificable, defecto o error que proporcione una visibilidad directa o indirecta de los objetivos o bienes dentro del canal y ámbito elegido (Herzog, 2003).

$$L_K = P_V$$

$$L_K = 1$$

e. ANOMALÍAS

Cuente cada elemento identificable o desconocido que no pueda tenerse en cuenta en las operaciones normales, por lo general cuando la fuente o el destino del elemento no se pueden entender. Una anomalía puede ser una señal temprana de un problema de seguridad. Dado que las incógnitas son los elementos que no pueden ser controlados, una auditoría adecuada requiere ir observando y anotando todas las anomalías (Herzog, 2003).

No se observaron anomalías durante el tiempo que se realizó el test de penetración, por lo tanto: $L_A = 0$

3.4.1.1.4 CÁLCULO DE RAVS

La forma más simple para hacer RAVs es usar las hojas de cálculo creadas específicamente para calcular el área de ataque y varias métricas requeridas a partir de los datos de prueba. Esta hoja de cálculo se encuentra disponible en el sitio web de ISECOM. El analista sólo necesita introducir los valores en las cajas blancas vacías, y el resto de los cálculos se manejará de forma automática (Herzog, 2003).

De acuerdo a los valores obtenidos en la seguridad operacional, controles y limitaciones, se ha realizado el cálculo; el mismo que se muestra en la **FIGURA 3. 4**

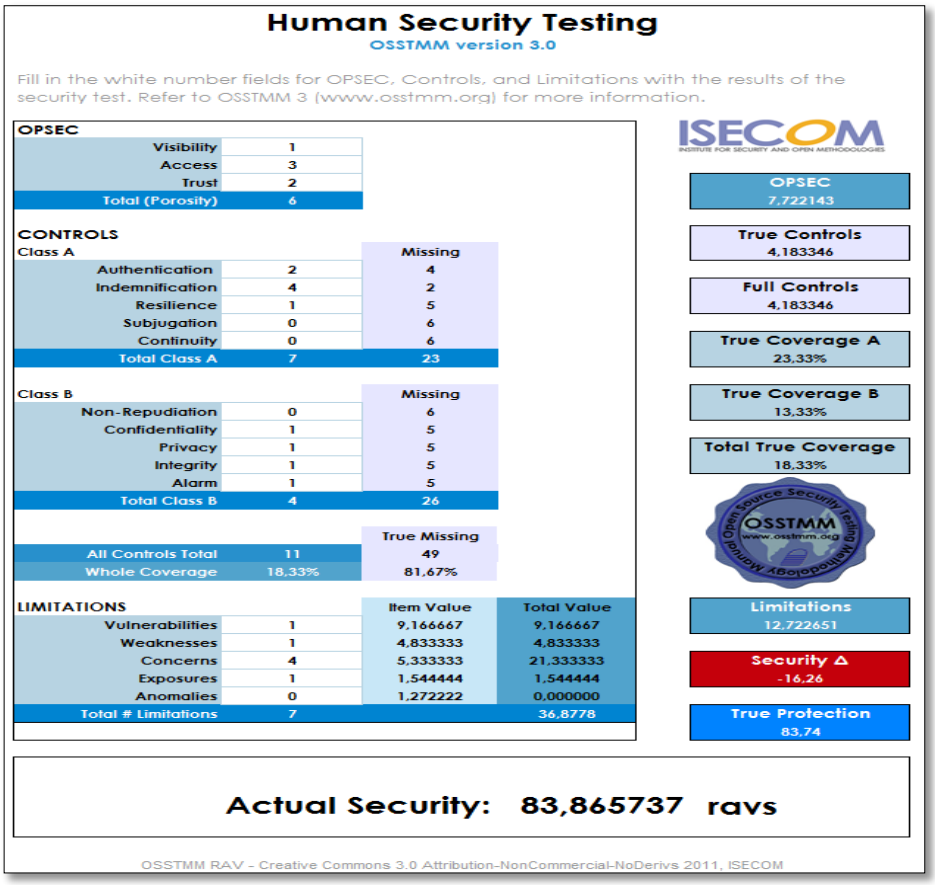


FIGURA 3. 4: Cálculo del RAVS en Canal Humano.

Fuente: Obtenida de la Calculadora de RAVs de OSSTMM 3.0

3.4.1.1.5 INTERPRETACIÓN DE RESULTADOS

La seguridad operacional es considerablemente baja, reflejada en la falta de manuales de normas y buenas prácticas del correcto uso de la información actualmente implementadas por la administración.

Se tiene un grado de prioridad alto en cuanto a la indemnización del personal, más no así en otros controles que son totalmente nulos como la Subyugación y la Continuidad.

Las limitaciones se consideran individualmente, pero éstas se relacionan directamente con algunos controles y seguridad operacional, es así que debido a ello se tiene limitaciones nulas como en el no repudio; y casi nulas en cuanto a confidencialidad, privacidad, integridad y alarma.

3.4.1.2 FÍSICO

El objetivo de realizar las pruebas de seguridad en este canal es intentar penetrar las barreas físicas y lógicas de la organización.

PHYSSEC (seguridad física) es una clasificación para la seguridad material en el reino físico que está dentro de los límites del espacio 3D humano-interactivo. Prueba de este canal requiere la interacción no-comunicativo con las barreras y los seres humanos en posiciones controlador de acceso de los activos. Este canal cubre la interacción del analista dentro de la proximidad de los objetivos (Herzog, 2003).

3.4.1.2.1 SEGURIDAD OPERACIONAL

A continuación se detalla cómo se obtuvieron los resultados de la seguridad operacional en el canal de seguridad física.

a. Visibilidad

Este es un método para evaluar la seguridad física de una organización y sus bienes, verificando las medidas de seguridad de su perímetro físico. En la **TABLA 3. 15** se muestran los resultados obtenidos en este canal.

- Trazar mapa del perímetro físico
- Trazar mapa de las medidas de protección físicas (cercas, puertas, luces, etc.)
- Trazar mapa de las rutas de acceso y/o métodos físicos
- Trazar mapa de las áreas no monitoreadas (Herzog, 2003)

TABLA 3. 15: Resultados obtenidos en Seguridad Operacional: Visibilidad

Resultados de Visibilidad		
Mapa del perímetro físico.	**Tipos de medidas de protección física.**	**Lista de áreas desprotegidas o insuficientemente protegidas. (P_V)**
Por motivos de confidencialidad, el mapa del perímetro físico no será mostrado en este documento.	Personal de guardianía. Alarma contra incendios.	Por motivos de confidencialidad, las áreas insuficientemente protegidas no serán mostradas en este documento.

Fuente: Desarrollo del proyecto

Después del análisis realizado el resultado de visibilidad es: P_V=3 debido a que existen tres lugares desprotegidos.

b. Accesos

Este es un método para evaluar los privilegios de acceso a una organización y a sus bienes a través de puntos de acceso físicos. En la **TABLA 3. 16** se muestran los resultados obtenidos de este test.

- Enumerar áreas de control de acceso.
- Examinar dispositivos y tipos de control de acceso.
- Examinar tipos de alarmas.
- Determinar el nivel de complejidad de un dispositivo de control de acceso.
- Determinar el nivel de privacidad en un dispositivo de control de acceso.
- Examinar los dispositivos de control de acceso en búsqueda de puntos débiles y vulnerabilidades.
- Examinar posibles ataques de denegación de servicio sobre los dispositivos de control de acceso.

TABLA 3. 16: Resultados obtenidos en seguridad operacional Accesos

Seguridad operacional- Acceso (P_A)		
Lista de puntos de acceso físico.	1.	Puertas
	2.	Ventanas
Tipos de autenticación.	3.	Biométrico
Tipos de sistemas de alarmas.	4.	Alarma contra incendios.

Fuente: Desarrollo del proyecto

El nivel de acceso en el canal “Físico” es de cuatro debido a que se consideró cuatro factores los mismos que se enumeran en la tabla anterior:

$$P_A:=4$$

c. Confianza

Es un método para obtener acceso a una organización o a sus bienes, a través de puntos débiles en su ubicación y en su protección contra elementos externos (Herzog, 2003).

1. Enumerar las áreas de la organización que son visibles.

Debido a que es una entidad financiera y está al servicio de la ciudadanía, existen 3 áreas visibles, ninguna compromete la seguridad de la información.

2. Enumerar las áreas dentro de la organización que son audibles.

Existen 6 lugares audibles que son visibles, los 6 están al servicio de la ciudadanía.

3. Examinar las áreas de la ubicación referentes a las entradas por abastecimiento y búsqueda de puntos débiles y vulnerabilidades.

Existen puntos débiles y vulnerabilidades, por motivos de confidencialidad no se mostrará su ubicación; pero en este caso se tiene una **confianza de 2**.

4. Listar las empresas y empleados de abastecimiento.

Se dispone proveedores de soporte y servicios que representan una vulnerabilidad debido al acceso que tienen a los activos dentro de la organización. Para este caso se tiene una **confianza de 3**.

5. Listar las empresas y empleados de limpieza.

Únicamente existe una persona encargada de la limpieza la cual puede significar un punto de vulnerabilidad debido al acceso que tiene a las diferentes áreas de la empresa. En este punto se tiene una **confianza de 1**.

El nivel de confianza en el canal “Físico” será la suma de todos los niveles de confianza obtenidos anteriormente: $\boldsymbol{P_T}$**= 6**.

3.4.1.2.2 CONTROLES

El siguiente paso en el cálculo de la RAV es definir los controles; los mecanismos de seguridad puestos en marcha para proteger las operaciones.

a. Autenticación

La medición de la amplitud y profundidad de los puntos de acceso interactivos dentro de la meta y la autenticación requerida. El punto de acceso es el punto principal de cualquier interacción entre activos. La verificación de un punto de acceso que existe es una parte de la determinación de su propósito (Herzog, 2003).

En este caso existe control de autenticación es 1 debido a que se utiliza el control de huella digital como registro más no como acceso.

$$LC_{Au}=1$$

b. Indemnización

Documentar y enumerar la capacidad de abusar o evadir la política de los empleados, de seguros, de no divulgación, no competencia.

- Enumerar el uso de señales de advertencia de peligro, vigilancia o alarmas en efecto, problemas de salud, y publicaciones de ninguna entrada.
- Verificar el alcance y la finalidad de la acción legal que se utiliza para mantener la indemnización.

En la **TABLA 3. 17** se muestran los resultados obtenidos de este test.

TABLA 3. 17: Resultados obtenidos en Control Indemnización.

Resultados Control indemnización	
Lista de señales de advertencia de peligro, vigilancia o alarmas en efecto, problemas de salud y publicaciones de ninguna entrada. **(LC_{Id})**	1. Existen pocas señales de emergencia. Existen garantías de activos físicos como: 2. Servidores, 3. Impresoras, 4. Software. Algunas de ellas ya han caducado.

Fuente: Desarrollo del proyecto

En este caso el control de indemnización en el canal físico es:

LC_{Id}=4; por lo mencionado en la tabla anterior.

c. Resistencia

La determinación y la medición de la capacidad de resistencia de las barreras y guardias en el ámbito de los cambios excesivos u hostiles diseñados para causar insuficiencia de operaciones (Herzog, 2003).

En la **TABLA 3. 18** se muestran los resultados obtenidos de este test.

TABLA 3. 18: Resultados obtenidos en Control Resistencia.

Resultados Control Resistencia	
Enumerar y verifique que la distracción, la eliminación o aquietamiento de personal no permitirán el acceso directo a los activos u operaciones.	Existe solo un guardia de seguridad a la entrada del edificio.
Resultados Control Resistencia	
Enumerar y verificar que la desactivación o destrucción de las medidas de seguridad o controles operacionales no permitirán el acceso directo a los activos u operaciones.	No permite
Compruebe que el aislamiento del alcance de los recursos como, la energía, el agua, las comunicaciones, etc. no permita el acceso directo a los activos u operaciones.	No permite
Ejemplo:	En una auditoria física cuando el control de 2 guardias de acceso a una puerta, si uno no está presente el otro no puede abrir la puerta, esto indica que existe resistencia.

Fuente: Desarrollo del proyecto

De acuerdo al test, el control de resistencia de: LC_{Re}=0 ya que no existe ningún mecanismo que presente resistencia.

d. Subyugación

Enumerar y probar deficiencias en acceso a los bienes no controlados por la fuente que proporciona el acceso (es decir, números PIN, fotografías de identificación, etc. seleccionados por parte del actor, inicios de sesión con los números de identificación escritas por parte del actor, etc) (Herzog, 2003).

De acuerdo al test, el control de subyugación es uno:

$$LC_{Su}= 1$$

Ya que algunos operarios tienen expuestas sus claves en lugares visibles.

e. Continuidad

En la **TABLA 3. 19** se muestran los resultados obtenidos en el control de continuidad realizado en la empresa.

TABLA 3. 19: Resultados obtenidos en Control Continuidad.

Resultados Control Continuidad	
Enumerar y verificar las condiciones en que los retrasos de acceso son abordados adecuadamente a través del personal de copia de seguridad o un medio automatizado para el acceso oportuno a los servicios, procesos y operaciones.	No se dispone de un sistema automatizado de copias de seguridad.
Verificar que el aislamiento del alcance a partir de recursos, tales como, energía eléctrica, alimentos, agua, comunicaciones, etc, no se detendrá o negará el acceso a los servicios, procesos y operaciones.	1. En este test, mediante observación directa se verificó el control de continuidad a partir de recursos importantes como el de energía eléctrica.
Verificar que la incapacidad para eliminar los residuos, contaminantes u otros contaminantes del ámbito de aplicación no detenga o deniegue el acceso a los servicios, procesos y operaciones.	2. En este test mediante observación directa se pudo verificar el control de continuidad a partir de la limpieza del cuarto de equipos.

Fuente: Desarrollo del proyecto

Por lo mencionado en la tabla anterior el control de continuidad es dos: LC_{Ct}= 2

f. No repudio

Enumerar y poner a prueba para su uso o insuficiencias de los monitores y sensores para identificar y registrar el acceso o las interacciones con los activos de pruebas específicas para desafiar repudio correctamente. Documentar la profundidad de la interacción que se registra (Herzog, 2003).

De acuerdo al test, el control de No-Repudio es nulo:

LC_{NR}=0 ya que no existe ningún control sobre esto.

g. Confidencialidad

Enumerar y probar el uso o deficiencias de todas las señales, la comunicación física, los elementos transportados internamente entre ambos, los procesos y el personal que utilicen códigos, lenguaje indescifrable, "tranquilizado" o "cerrado" las interacciones personales para promover la confidencialidad de la comunicación sólo a los que tienen el correcto control de seguridad de esa comunicación clasificada.

De acuerdo al test, el control de Confidencialidad es:

LC_{Cf} = 0 ya que no existe un control de confidencialidad en una comunicación física.

h. Privacidad

Enumerar y probar el uso o insuficiencias de todas las interacciones dentro del alcance utilizando etiquetado no evidente a las interacciones hacia el “cuarto cerrado", y dentro de cuartos elegidos al azar para ocultar o proteger la privacidad de la interacción sólo a los que tienen la habilitación apropiada de seguridad para ese proceso o activo (Herzog, 2003).

El control de privacidad en este canal es LC_{Pr}=2 por los siguientes motivos:

1. Se utiliza etiquetado no evidente de los activos.
2. Los activos son almacenados en un lugar apartado para proteger la privacidad de los mismos.

i. Integridad

En la **TABLA 3. 20** se muestran los resultados obtenidos en el control de integridad.

TABLA 3. 20: Resultados obtenidos en Control Integridad.

RESULTADOS CONTROL INTEGRIDAD	
Tipo de test	Observación directa
Enumerar y probar las deficiencias de todas las señales y la comunicación entre procesos y personal que utiliza un proceso documentado, sellos, firmas digitales, o marcas cifradas para proteger y asegurar que los activos no pueden ser cambiados, redirigidos, o invierten sin que sean conocidas las partes involucradas en el acceso a todos los lugares. (LC_{NR})	1. Todos los documentos que se transmiten internamente en la cooperativa, tienen sello y firma, por parte de los emisores y receptores; así como de terceras personas que intervengan en el proceso de transporte de los mimos.
Verificar que todos los medios de almacenamiento de información no estén en peligro de la descomposición natural, tales como daños por el calor o la humedad, decoloración por la exposición directa de la luz solar, o la degradación magnética.	Sólo pocos medios de almacenamiento cumplen con las medidas de protección contra daños naturales.

Fuente: Desarrollo del proyecto

De acuerdo a los datos mostrados en la tabla anterior, el control de Integridad es: LC_{NR}=1

j. Alarma

Verificar y enumerar el uso de un sistema de alerta localizada o en todo el ámbito de aplicación, inicio de sesión o mensaje para cada pasarela de acceso cuando una situación sospechosa es observada por el personal en caso de sospecha de intentos de elusión, la actividad fraudulenta, violación o incumplimiento. Asegúrese de que los sensores / sistemas se instalan a las normas nacionales, regionales o internacionales y probados con regularidad para cubrir todos los puntos accesibles (Herzog, 2003).

En la **TABLA 3. 21** se muestran los resultados obtenidos en este control.

TABLA 3. 21: Resultados obtenidos en Control Alarma.

Resultados control alarma	
Tipo de test	Observación directa
Observaciones (LC_{Al})	No se dispone de un sistema de alarmas contra intrusiones.

Fuente: Desarrollo del proyecto

De acuerdo a los datos mostrados en la tabla anterior, el control de Alarma es: LC_{Al}=0

3.4.1.2.3 LIMITACIONES

El siguiente paso, es el cálculo de las limitaciones; las mismas que están consideradas de forma individual.

a. Vulnerabilidad

En la seguridad física, una vulnerabilidad puede ser tan simple como una puerta de cristal, una puerta de metal corroído por el tiempo, una puerta que se puede cerrar por acuñando de monedas en la brecha entre él y su marco, los equipos electrónicos no sellada partir plagas como las hormigas o ratones, una unidad de CD de arranque en un PC, o un proceso que permite a un empleado para tomar un bote de basura lo suficientemente grande como para ocultar o transporte activos fuera del ámbito de aplicación (Herzog, 2003).

Por motivos de confidencialidad no se enumera las vulnerabilidades.

De acuerdo al test, las vulnerabilidades son:

$$L_V=7$$

b. Debilidad

En seguridad física, una debilidad puede ser una cerradura de la puerta que se abre cuando una tarjeta se acuña entre éste y el marco de la puerta, un generador eléctrico de respaldo sin combustible, o un seguro que no cubre los daños por inundaciones en una zona de inundación (Herzog, 2003). En la **TABLA 3. 22** se muestran ejemplos de algunas debilidades que se encontraron y que por motivos de seguridad no se muestran.

TABLA 3. 22: Resultados obtenidos en la limitación debilidad.

Resultados Limitación debilidad	
Tipo de test	Observación directa
Observaciones (L_V)	• Existen garantías de equipos caducadas. L_V= 2 • Licencias de software caducadas. L_V= 3 • Uso de sistemas operativos sin soporte como XP. L_V= 1

Fuente: Desarrollo del proyecto

De acuerdo al test, el cálculo de las debilidades es la suma de los controles mostrados en la tabla anterior: L_V= 6

c. Preocupación

En seguridad física, una preocupación puede ser un mecanismo de bloqueo de la puerta cuyos controles y tipos de operación son clave pública, un generador de respaldo sin medidor de potencia o indicador de combustible, un proceso de equipo que no requiere que el empleado firme la salida de materiales cuando se reciben, o una alarma de fuego no lo suficientemente fuerte para ser escuchado por los trabajadores de maquinaria que deban usar tapones para los oídos (Herzog, 2003).

Cuente cada defecto o error en los controles del proceso: el no repudio, confidencialidad, privacidad, integridad y alarma.

$$L_c = LC_{Cf} + LC_{Al} + LC_{It} + LC_{Pr} + LC_{NR}$$

$$L_c = 0+0+1+2+0$$

$$L_c = 3$$

d. Exposición

Cuente cada acción injustificable, defecto o error que proporciona una visibilidad directa o indirecta de los objetivos o bienes dentro del canal ámbito elegido.

$$L_K = P_V = 3$$

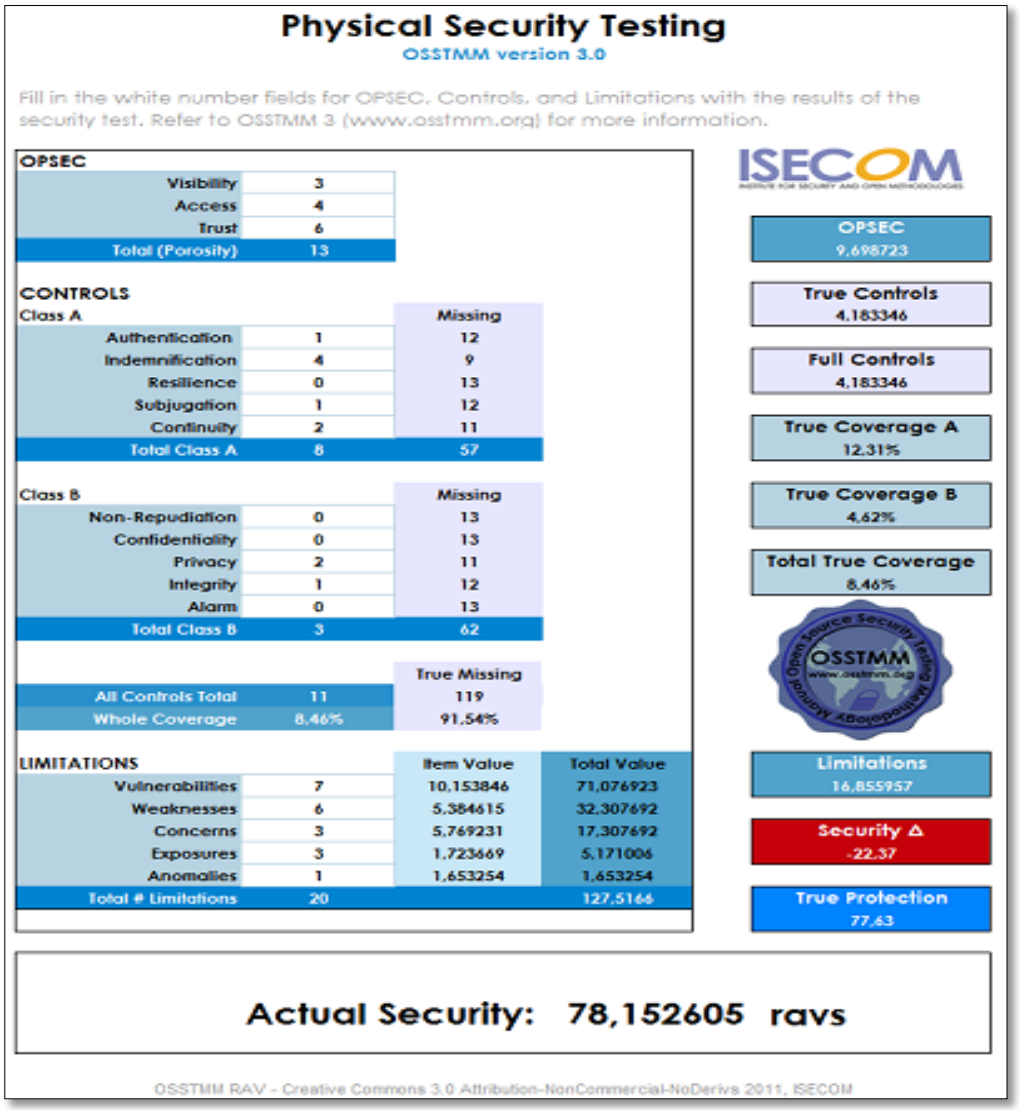
e. Anomalías

En seguridad física una anomalía puede ser pájaros muertos descubiertos en el techo de un edificio en torno a los equipos de comunicaciones.

$$L_A = 1$$

3.4.1.2.4 CÁLCULO DE RAVS

Una manera directa y más simple para hacer RAVs es usar las hojas de cálculo creadas específicamente calcular el área de ataque y varias métricas requeridas, populares a partir de los datos de prueba. El analista sólo necesita introducir los valores en las cajas blancas vacías, y el resto de los cálculos se manejará de forma automática (Herzog, 2003). El mismo que se muestra en la **FIGURA 3. 5**



.

FIGURA 3. 5: Cálculo del RAVS en Canal Seguridad Física

Fuente: Calculadora de RAVs OSSTMM

3.4.1.2.5 INTERPRETACIÓN DE RESULTADOS

Al realizar el test de seguridad física y analizar los controles existentes se determinó que lamentablemente no se tiene implementados algunos controles de seguridad física los mismos que resultan un blanco perfecto para los atacantes informáticos.

Las limitaciones se analizan individualmente, pero éstas están relacionadas con algunos controles, de tal forma como los valores en seguridad operacional son relativamente altos, estos valores influyen para que el cálculo de las limitaciones sea también relativamente alto. Como resultado se obtiene una gran preocupación debido a que se tiene una limitación de vulnerabilidad muy alta en relación a los demás parámetros.

3.4.2 SEGURIDAD DE COMUNICACIONES

En el canal de seguridad de comunicaciones interviene la sección de telecomunicaciones y la de redes de datos, en los cuales se tendrán que evaluar los diferentes módulos de los 4 puntos de interacción que involucran al proceso de OSSTMM.

3.4.2.1 TELECOMUNICACIONES

Comprende todas las redes de telecomunicación, digital o analógica, donde la interacción se lleva a cabo a través de los teléfonos y las líneas telefónicas (Herzog, OSSTMM 3.0, 2003).

Tiene como objetivo monitorear las telecomunicaciones; mediante pruebas de controles a nivel de red para bloquear actividades no autorizadas y las respuestas de registro y tiempo de respuesta, como los filtros de acceso basados en llamadas de teléfono (CLID), de direcciones de red de usuario (NUA), o grupo cerrado de usuarios (CUG) y mediante pruebas de controles a nivel de aplicación; verificando que están en su lugar para bloquear actividades no autorizadas y las respuestas de registro y tiempo de respuesta.

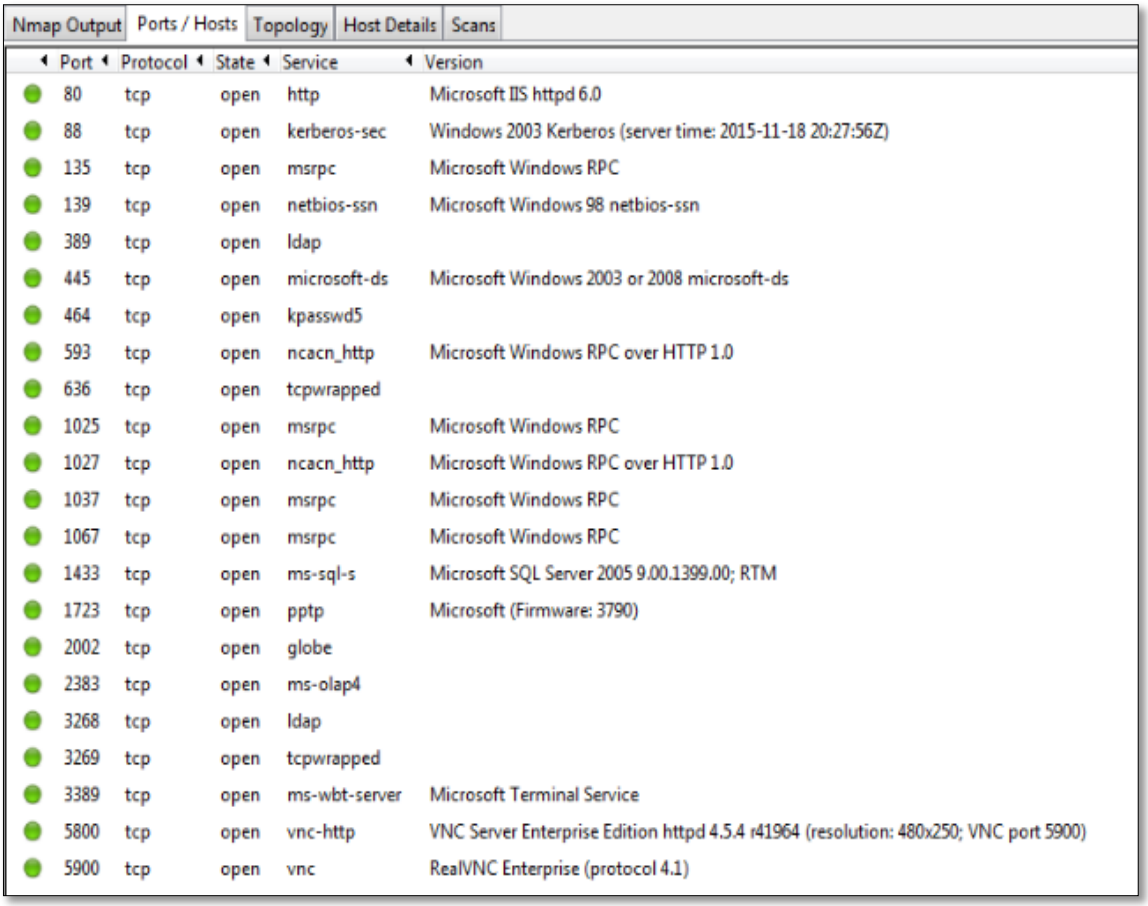
3.4.2.1.1 SEGURIDAD OPERACIONAL

A continuación, se detalla cómo se obtuvieron los resultados de la seguridad operacional en el canal de seguridad de las telecomunicaciones.

a. Visibilidad

1. Enumeración e indexación de los objetivos en el ámbito de aplicación a través de la interacción directa e indirecta incluso con entre los sistemas directo. P_V= 1.
2. Realizar un mapa de los protocolos de comunicación en uso dentro del ámbito de aplicación.

Utilizando el software Zenmap se realizó un escaneo de puertos, y en la **FIGURA 3. 6** se puede evidenciar un resumen de algunos de los puertos más conocidos dentro del ámbito de aplicación. P_V= 1



Port	Protocol	State	Service	Version
80	tcp	open	http	Microsoft IIS httpd 6.0
88	tcp	open	kerberos-sec	Windows 2003 Kerberos (server time: 2015-11-18 20:27:56Z)
135	tcp	open	msrpc	Microsoft Windows RPC
139	tcp	open	netbios-ssn	Microsoft Windows 98 netbios-ssn
389	tcp	open	ldap	
445	tcp	open	microsoft-ds	Microsoft Windows 2003 or 2008 microsoft-ds
464	tcp	open	kpasswd5	
593	tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
636	tcp	open	tcpwrapped	
1025	tcp	open	msrpc	Microsoft Windows RPC
1027	tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
1037	tcp	open	msrpc	Microsoft Windows RPC
1067	tcp	open	msrpc	Microsoft Windows RPC
1433	tcp	open	ms-sql-s	Microsoft SQL Server 2005 9.00.1399.00; RTM
1723	tcp	open	pptp	Microsoft (Firmware: 3790)
2002	tcp	open	globe	
2383	tcp	open	ms-olap4	
3268	tcp	open	ldap	
3269	tcp	open	tcpwrapped	
3389	tcp	open	ms-wbt-server	Microsoft Terminal Service
5800	tcp	open	vnc-http	VNC Server Enterprise Edition httpd 4.5.4 r41964 (resolution: 480x250; VNC port 5900)
5900	tcp	open	vnc	RealVNC Enterprise (protocol 4.1)

FIGURA 3. 6: Mapa de los protocolos de comunicación.
Fuente: Obtenida del software Zenmap

3. Esquema de la topología de las redes de telecomunicaciones.

La topología de red de la cooperativa es una topología plana, es decir no está segmentada o jerarquizada, la misma cuenta con varios dispositivos de red, como conmutadores, enrutadores y servidores; enlazados con cable UTP Cat 6. P_V= 1.

La **FIGURA 3. 7** que se presenta, es una representación de la topología de red de la cooperativa, es importante aclarar que ha sido modificada de la original por motivos de seguridad.

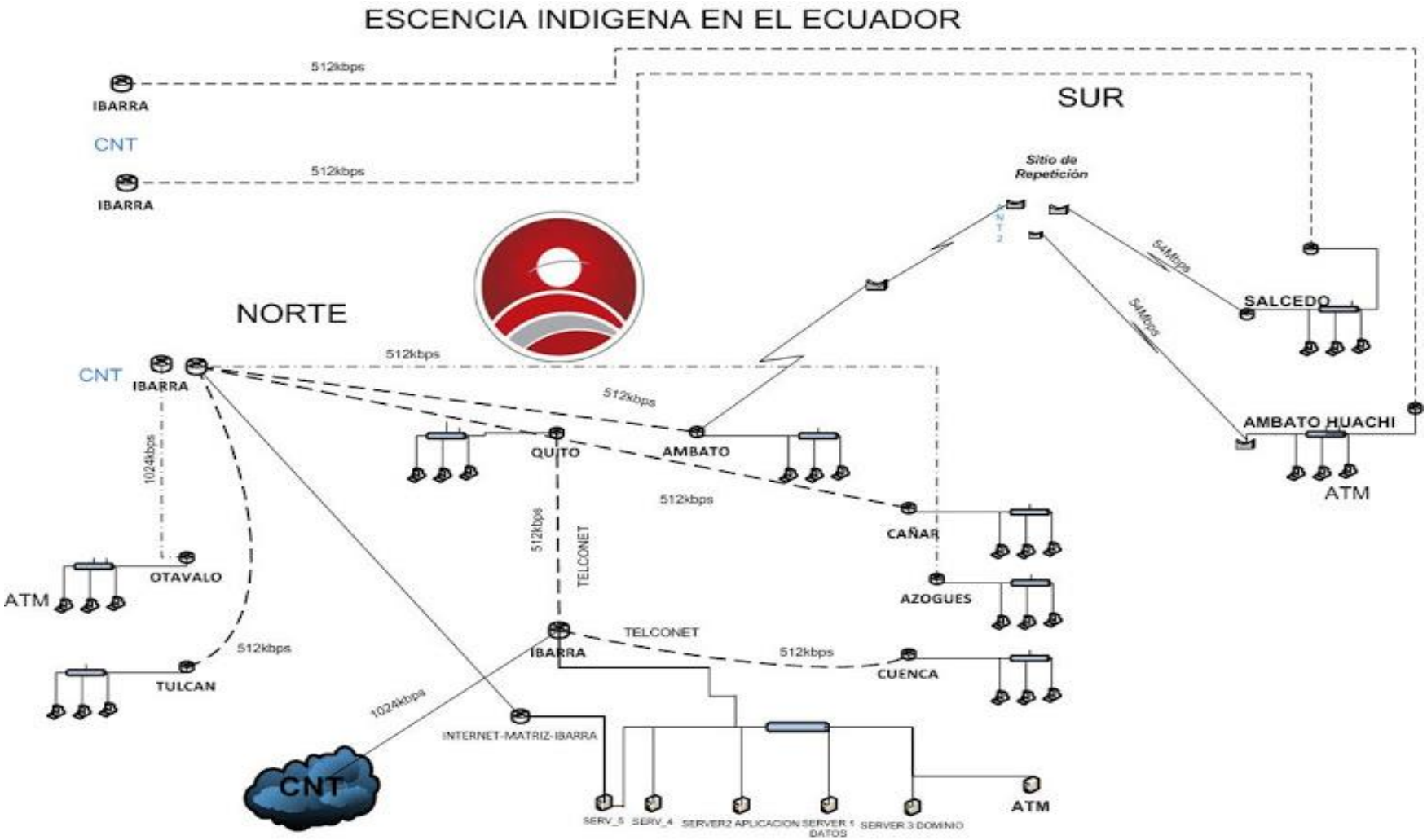


FIGURA 3. 7: Topología de red de la empresa.

Fuente: Cooperativa Escencia Indígena

4. Identificar los tipos de sistemas operativos y versiones en uso en sistemas dentro del ámbito de aplicación.

Con la utilización del software Zenmap, se pudo determinar los sistemas operativos utilizados en host y servidores de la red de datos de la cooperativa.

En la **FIGURA 3. 8** se puede observar un fragmento de los resultados obtenidos por dicho software, recalcando que la imagen ha sido editada por motivos de seguridad. P_V= 1

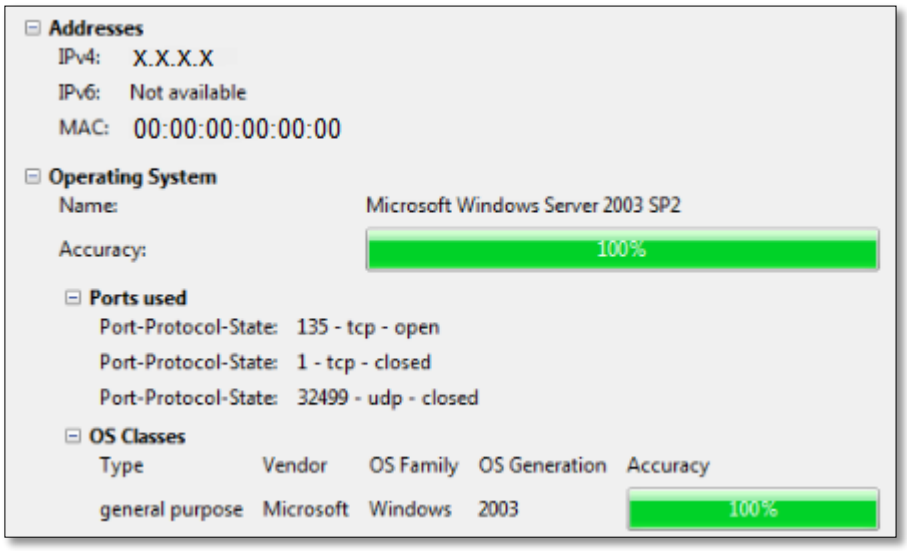


FIGURA 3. 8: Identificación de sistemas operativos y aplicaciones.

Fuente: Obtenida del software Zenmap.

Después del análisis realizado el resultado de visibilidad es: P_V= 4 debido a que han sido evaluados 4 aspectos que representan visibilidad.

b. Accesos

Las pruebas para la medición de la amplitud y profundidad de los puntos de acceso interactivos líderes en el ámbito y la autenticación requerida.

1. Relacionar cada puerto abierto con un servicio y protocolo.

Con el mapa de puertos descrito en el área de Visibilidad, se puede relacionar los servicios con dichos puertos. P_A= 1

2. Verificar la aplicación y su versión en el sistema.

Dicha información fue obtenida mediante observación directa en la cooperativa y su información no será revelada por motivos de confidencialidad. P_A= 1

3. Identificar los componentes de los servicios en escucha.

Mediante el snnifer Wireshark se identificó los componentes de los servicios.

El nivel de acceso en el canal "Telecomunicaciones" es de tres debido a que se realizaron tres pruebas en las cuales todas representaron un acceso: P_A= 1

$$P_A = 3$$

c. Confianza

Para una auditoría de Telecomunicaciones de redes de datos, el auditor cuenta cada tipo de servicio abierto o puerto abierto como una Confianza (Herzog, 2003).

En este caso, se debe realizar un análisis de los puertos que están abiertos y los que están cerrados, y el porqué de su estado. Ya que no es posible que todos los puertos se encuentren cerrados debido a la necesidad de acceder a ciertas aplicaciones; y tampoco que todos estén abiertos debido a las vulnerabilidades que se expone la red.

El nivel de confianza en el canal "Telecomunicaciones" es de 22 ya que se encontró 22 puertos abiertos: P_T= 22.

3.4.2.1.2 CONTROLES

El siguiente paso en el cálculo de la RAV es definir los controles; los mecanismos de seguridad puestos en marcha para proteger las operaciones.

a. Autenticación

1- Enumerar los recursos de telecomunicaciones que requieren autenticación y verificar todas las formas aceptables de privilegios para interactuar o recibir acceso.

Existen controles de autenticación y privilegios de acceso. $\boldsymbol{LC_{Au} = 2}$

2- Asegurarse que las cuentas administrativas no tengan la contraseña por defecto o fáciles de adivinar, para su acceso.

Las contraseñas de las cuentas administrativas no son por defecto y son muy robustas. $\boldsymbol{LC_{Au} = 2}$

3- Asegurarse que las cuentas de usuario no tengan la contraseña por defecto o fáciles de adivinar, para su acceso.

Las contraseñas de las cuentas de usuario no son por defecto. $\boldsymbol{LC_{Au} = 1}$

4- Verificar la información de autenticación cuando se realiza un intento de acceso, si es exitoso o fallido (Herzog, 2003).

Se tiene un número limitado de intentos de acceso, si se falla el sistema se bloquea automáticamente. $\boldsymbol{LC_{Au} = 1}$

En este caso el control de autenticación es la suma de los valores antes mostrados: LC_{Au}=6

b. Indemnización

❖ Verificar la legalidad y el lenguaje adecuado en las limitaciones de responsabilidad.

Se verifico el lenguaje utilizado en todas las actas de responsabilidad que se entregan en la empresa y resultó ser claro y adecuado.

1. Actas de entrega de equipos informáticos.

2. Actas de responsabilidad de equipos informáticos.

3. Acuerdo de responsabilidad de información reservada de la empresa. $\boldsymbol{LC_{Au} = 3}$

❖ Examinar el lenguaje de la póliza de seguro para las limitaciones en los tipos de daños en los activos de la empresa.

1. Se firman contratos de garantía que cubren daños y robos de los activos de telecomunicaciones. $\boldsymbol{LC_{Au} = 1}$

En este caso el control de indemnización en el canal Telecomunicaciones es la suma de todos los valores antes mencionados:LC_{Au}=4

c. Resistencia

Mapa y documentos en el proceso de porteros desconectando canales por incumplimiento o dudas de seguridad como un análisis de las carencias con reglamentación y política de seguridad (Herzog, 2003).

De acuerdo al test, el control de resistencia es cero ya que no existe ningún control de los antes mencionados: LC_{Re}=0

d. Subyugación

Enumerar y poner a prueba las insuficiencias de todos los canales a utilizar o permitir controles de pérdida no habilitados de forma predeterminada (Herzog, 2003).

De acuerdo al test aplicado, el control de subyugación es:LC_{Su}=0

e. Continuidad

TABLA 3. 23: Resultados obtenidos en Control Continuidad.

Resultados control de Continuidad	
Tipo de test	Observación directa
Enumerar y probar las deficiencias de todos los objetivos en materia de retrasos de acceso y los tiempos de respuesta de servicio a través de los sistemas de back-up o el interruptor de canales alternos.	En el test realizado se pudo evidenciar que existe un solo control de continuidad y es el respaldo de energía eléctrica en el caso de interrupción.

Fuente: Desarrollo del proyecto

Por lo tanto el control de continuidad es:

$$LC_{Ct}=1$$

f. No repudio

- Enumerar y probar para su uso o insuficiencias de demonios y de los sistemas de identificación y registro de acceso o las interacciones con la propiedad para pruebas específicas para desafiar repudio correctamente.

- Documento de la profundidad de la interacción grabada y el proceso de identificación.

- Verifique que todos los métodos de interacciones se registran correctamente con la identificación apropiada.

- Identificar métodos de identificación que derrota de repudio (Herzog, 2003).

De acuerdo al test, el control de No-Repudio es:

$$LC_{NR}=0$$

Este control es cero debido a no encontrarse ningún resultado en ninguno de los test realizados.

g. Confidencialidad

- Enumerar todas las interacciones con los servicios en el ámbito de las comunicaciones o bienes transportados por el canal mediante líneas seguras, cifrado, interacciones para proteger la confidencialidad de la propiedad de la información entre las partes involucradas.

- Verificar los métodos aceptables utilizados para la confidencialidad.

- Prueba de la resistencia y el diseño del método de cifrado o la ofuscación.

- Verificar los límites exteriores de la comunicación que se pueden proteger a través de los métodos aplicados o confidencialidad (Herzog, 2003).

De acuerdo al test, el control de Confidencialidad es:

LC_{Cf}=1 ya que se usa cifrado para las comunicaciones externas.

h. Privacidad

- Enumerar los servicios en el ámbito de las comunicaciones o bienes transportados utilizando, firmas individuales específicos, identificación personal, interacciones personales para proteger la privacidad de la interacción y el proceso de suministro de bienes sólo para aquellos dentro de la debida autorización de seguridad para ese proceso, la comunicación, o de activos.

No existen servicios de firmas digitales para proteger la privacidad de las de las comunicaciones, pero si se cuenta con privacidad por parte de 3 proveedores de servicios y en la comunicación entre agencias. $\boldsymbol{LC_{Pr} = 4}$

- Relacionar información con los puertos que no responden para determinar si la disponibilidad depende de un tipo particular de contacto o protocolo.

Se encontró tres puertos que no responden adecuadamente. $\boldsymbol{LC_{Pr} = 3}$

De acuerdo al test, el control de Privacidad es la suma de los valores antes mencionados LC_{Pr}: = 7

i. Integridad

En la **TABLA 3. 24** se muestran los resultados obtenidos en el control de integridad.

TABLA 3. 24: Resultados obtenidos en Control Integridad.

Resultados Obtenidos en el control Integridad	
Tipo de test	Observación directa
Enumerar y probar las deficiencias de integridad donde utilizando un proceso documentado, firmas, cifrado, hachís, o marcas para asegurar que el activo no se puede cambiar, redirigido, o se invierte sin que se conoce a las partes involucradas. ($\boldsymbol{LC_{It}}$)	1. Los documentos, oficios o memorandos transmitidos internamente no se transmiten digitalmente; se lo hace físicamente y cada uno de ellos cuenta con sello y firma, pero no cuenta como un control de integridad.

Fuente: Desarrollo del proyecto

De acuerdo a lo expuesto en la tabla anterior, el control de Integridad es:

$$LC_{It}=1$$

j. Alarma

Verificar y enumerar el uso de un sistema de alerta localizada o en todo el ámbito de aplicación, registro, o un mensaje para cada pasarela de acceso a través de cada canal en una situación sospechosa es observada por el personal en caso de sospecha de intento de evasión, la ingeniería social, o la actividad fraudulenta (Herzog, 2003). Los resultados se indican en la **TABLA 3. 25**

TABLA 3. 25: Resultados obtenidos del control Alarma.

Resultados Obtenidos en el control Alarma	
Tipo de test	Observación directa
Observaciones (LC_{Al})	1. Cuando existen alarmas emitidas por analizador de red, el administrador actúa de la mejor manera ante dicha alarma.

Fuente: Desarrollo del proyecto

De acuerdo al test, el control de Alarma es: LC_{Al}=1

3.4.2.1.3 LIMITACIONES

El siguiente paso, es el cálculo de las limitaciones; las mismas que están ponderadas de forma individual.

a. Vulnerabilidad

En seguridad de las telecomunicaciones, una vulnerabilidad puede ser, una cabina telefónica que permite a cualquier persona acceder a la línea de teléfono de otra persona, un sistema de correo de voz que ofrece mensajes de cualquier teléfono en cualquier lugar, o una máquina de fax que se pueden sondear de forma remota para volver a enviar la última cosa en la memoria para el número del llamante (Herzog, 2003).

De acuerdo al test, las vulnerabilidades son dos ya que se tiene dos aspectos que representan vulnerabilidad pero no se describen por motivos de seguridad:

$$L_V=2$$

b. Debilidad

En seguridad de las telecomunicaciones, una debilidad puede ser un PBX que todavía tiene las contraseñas administrativas por defecto o un banco de módem para el acceso remoto de acceso telefónico en el que no registra el número de llamadas, hora y duración (Herzog, 2003).

En la **TABLA 3. 26** se muestran los resultados obtenidos en esta limitación.

TABLA 3. 26: Resultados obtenidos en Limitación Debilidad.

Resultados Obtenidos en la limitación Debilidad	
Tipo de test	Observación directa
Observaciones	1. Contraseña por defecto 2. Existe una mini central telefónica la cual no está correctamente administrada. 3. No se lleva un control de número de llamadas, hora y duración.

Fuente: Desarrollo del proyecto

De acuerdo a los resultados mostrados en la tabla anterior, el cálculo de las debilidades es: L_V= 3

c. Preocupación

En seguridad de las telecomunicaciones, una preocupación puede ser el uso de una máquina de FAX para el envío de información privada o un sistema de correo de voz que utiliza tonos táctiles para la introducción de un PIN o contraseña (Herzog, 2003).

Cuente cada defecto o error en los controles del proceso: el no repudio, confidencialidad, privacidad, integridad y alarma.

$$L_C = LC_{Cf} + LC_{Al} + LC_{It} + LC_{Pr} + LC_{NR}$$

$$L_C = 1+1+1+7+0$$

$$L_C = 10$$

d. Exposición

En seguridad de las telecomunicaciones, una exposición puede ser un directorio automatizado empresa ordenada alfabéticamente, lo que permite que cualquiera pueda desplazarse por todas las personas y números, o una máquina de fax que almacena los últimos números marcados.

Cuente cada injustificable acción, defecto o error que proporciona una visibilidad directa o indirecta de los objetivos o bienes dentro del canal ámbito elegido (Herzog, 2003).

$$L_K = P_V = 4$$

e. Anomalías

En seguridad de las telecomunicaciones, una anomalía puede ser una respuesta del módem desde un número que no tiene módem (Herzog, 2003).

$$L_A=0$$

3.4.2.1.4 CÁLCULO DE RAVS

Como ya se mencionó en apartados anteriores la manera más sencilla de calcular los RAVs es usando las hojas de cálculo que ofrece la metodología. Los resultados obtenidos en este canal se presentan en la **FIGURA 3. 9**

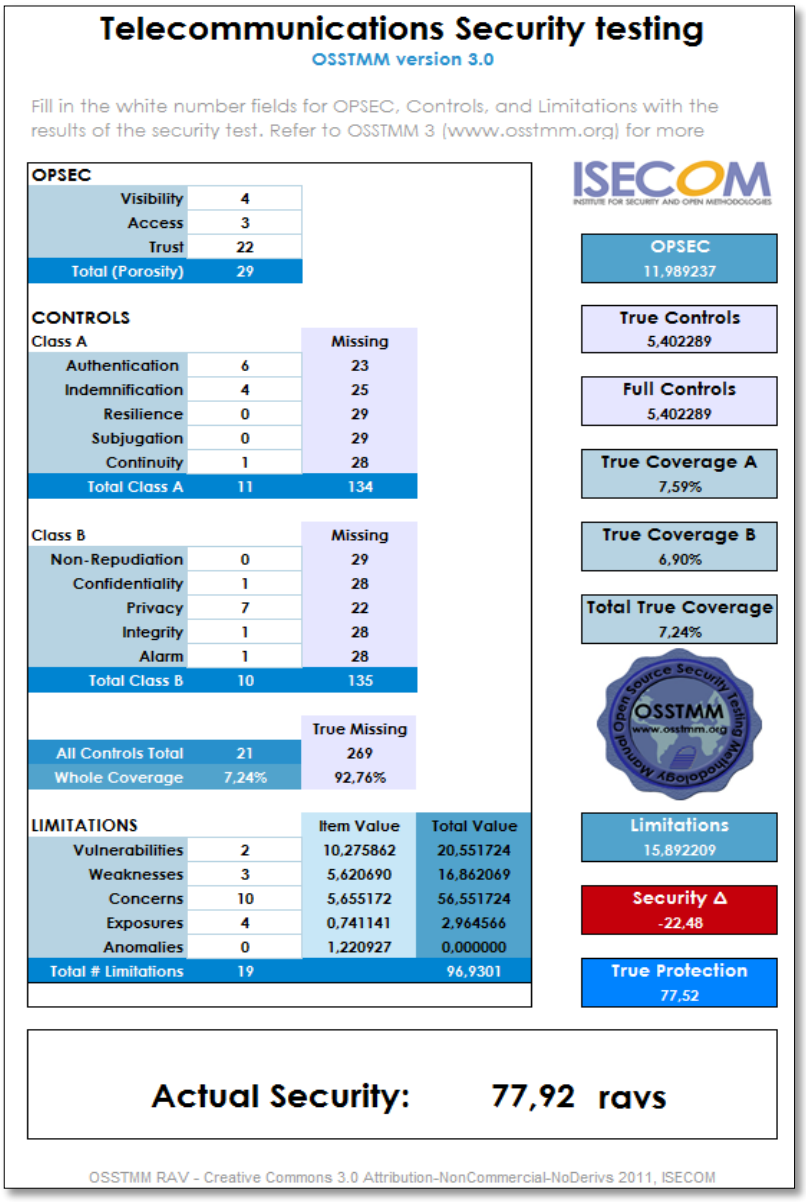


FIGURA 3. 9: Cálculo del RAVS en Canal Telecomunicaciones.

Fuente: Obtenida de la Calculadora de RAVs de OSSTMM 3.0

3.4.2.1.5 INTERPRETACIÓN DE RESULTADOS

La seguridad operacional es alta, principalmente en el aspecto de confianza, en el que se ha considerado todos los puertos que están abiertos, analizando el porqué de su estado.

Los controles son un mecanismo de seguridad puesto en marcha para proteger las operaciones, de acuerdo al test realizado, se tienen únicamente controles de Indemnización, autenticación y privacidad; los demás controles son nulos; abriendo una brecha para la inseguridad de la información.

Las limitaciones se valoran individualmente pero están relacionadas con algunos controles y seguridad operacional, debido a que los valores en seguridad operacional son altos, el cálculo de las limitaciones también lo es. Por lo tanto resaltan limitaciones como las Vulnerabilidades, debilidades y exposiciones las mismas que reflejan una administración no adecuada que expone a la red a ciertas amenazas informáticas.

3.4.2.2 REDES DE DATOS

Comprende todos los sistemas y redes de datos electrónicos donde la interacción se lleva a cabo a través de redes de datos cableados (Herzog, OSSTMM 3.0, 2003).

Tiene como objetivo monitorear los datos de entrada y salida de la red de comunicaciones a través de web, mensajería instantánea, chat, foros de discusión basados en la Web, o por e-mail, con la finalidad de verificar si consigo traen códigos maliciosos, conductas inapropiadas.

3.4.2.2.1 SEGURIDAD OPERACIONAL

Seguridad Operacional, también conocida como la porosidad del alcance, es el primero de los tres factores de la seguridad real que deberían determinarse. Se mide inicialmente como la suma de la visibilidad del alcance P_V, de acceso P_A, y la confianza P_T (Herzog, 2003). A continuación se detalla cómo se obtuvieron los resultados de la seguridad operacional en el canal red de datos.

a. Visibilidad

Enumeración e indexación de los objetivos en el ámbito de aplicación a través de la interacción directa e indirecta entre los sistemas directos.

- El uso de sniffing de red para identificar los protocolos que emanan respuesta de los servicios de red o peticiones en su caso. Por ejemplo, Netbios, ARP, SAP, NFS, BGP, OSPF, MPLS, RIPv2, etc.

En la **FIGURA 3. 10** se observa un extracto de uno de los escaneo, se ha editado tanto la dirección IP y MAC utilizada por motivos de seguridad. $\boldsymbol{P_V}$**=1**

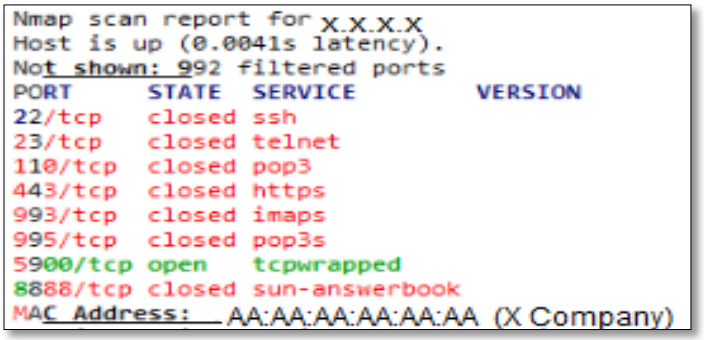


FIGURA 3. 10: Escaneo de red

Fuente: Obtenida del software Zenmap

- Consulta todos los servidores de nombres y los servidores de nombres del ISP o proveedor de alojamiento, así como la capacidad para realizar las transferencias de zona para determinar la existencia de todos los objetivos de la red y cualquier descuido relacionado, balanceo de carga, almacenamiento en caché, proxies, y de hosting virtual. $\boldsymbol{P_V}$**=18**. Los resultados se muestran en la **FIGURA 3. 11**

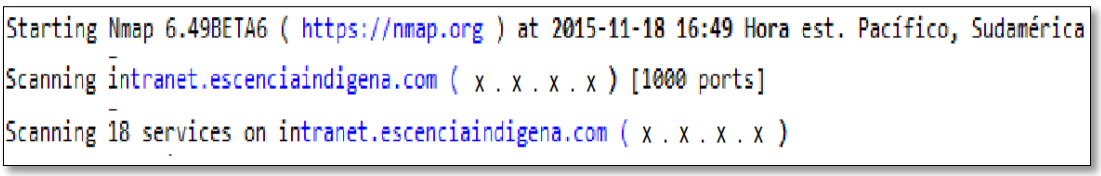


FIGURA 3. 11: Escaneo de servidores.

Fuente: Obtenida del software Zenmap

- Verificar y examinar el uso de protocolos de enrutamiento de tráfico y para todos los destinos.

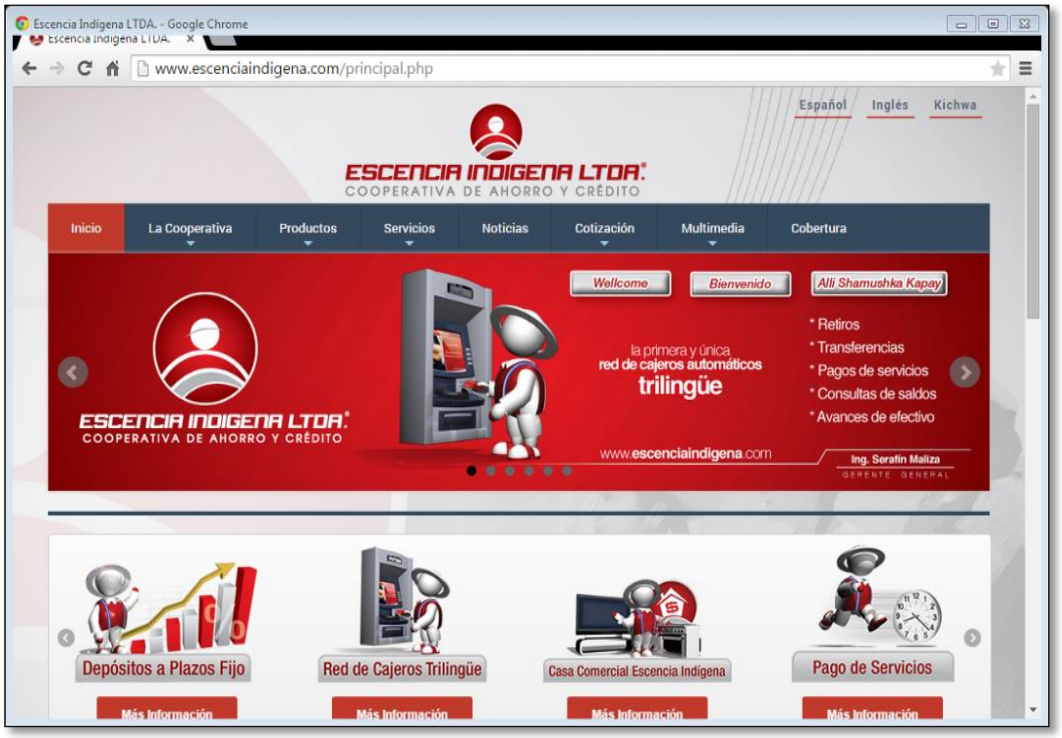
No están configurados protocolos de enrutamiento.

- Verificar defecto y probables nombres de comunidad SNMP en uso están de acuerdo con la práctica despliegues de todas las versiones de SNMP.

❖ Buscar los grupos de noticias, foros, IRC, IM, P2P, VoIP y comunicaciones basadas en la web para la conexión de datos del objetivo para determinar los sistemas de puerta de enlace de salida y direccionamiento interno.

La dirección Web de la página inicial de la empresa es:

http://www.escenciaindigena.com**,** la información proporcionada está relacionada a información de los productos, servicios y ofertas que presta en el sector financiero. Se muestra en la **FIGURA 3. 12**



.

FIGURA 3. 12: Página oficial de la empresa.

Fuente: Extraída de http://www.escenciaindigena.com

Se indagó a la vez de la información proporcionada mediante los dominios de Internet "escenciaindigena.com" en la base de datos Whois. P_V**=1.** Los resultados se muestran en la **FIGURA 3. 13**

```
Domain Name: ESCENCIAINDIGENA.COM
Registry Domain ID: 1646863540_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.enom.com
Registrar URL: www.enom.com
Updated Date: 2015-03-23T11:14:48.00Z
Creation Date: 2011-03-22T21:50:00.00Z
Registrar Registration Expiration Date: 2016-03-22T21:50:56.00Z
Registrar IANA ID: 48
Domain Status: clientTransferProhibited
Registry Registrant ID:
Registrant Name: DAVID GUEVARA AULESTIA
Registrant Organization: DDLINUX
Registrant Street: CALLE LA NI?A 0166 Y LOS SHYRIS
Registrant City: AMBATO
Registrant State/Province: TUNGURAHUA
Registrant Postal Code: 000000
Registrant Country: EC
Registrant Phone: +593.2840827
Registrant Phone Ext:
Registrant Fax: +593.2840827
Registrant Fax Ext:
Registrant Email: DAVID@DDLINUX.COM
Registry Admin ID:
Admin Name: DAVID GUEVARA AULESTIA
Admin Organization: DDLINUX
Admin Street: CALLE LA NI?A 0166 Y LOS SHYRIS
Admin City: AMBATO
Admin State/Province: TUNGURAHUA
Admin Postal Code: 000000
Admin Country: EC
Admin Phone: +593.2840827
Admin Phone Ext:
Admin Fax: +593.2840827
Admin Fax Ext:
Admin Email: DAVID@DDLINUX.COM
Registry Tech ID:
Tech Name: DAVID GUEVARA AULESTIA
Tech Organization: DDLINUX
Tech Street: CALLE LA NI?A 0166 Y LOS SHYRIS
Tech City: AMBATO
Tech State/Province: TUNGURAHUA
Tech Postal Code: 000000
Tech Country: EC
Tech Phone: +593.2840827
Tech Phone Ext:
Tech Fax: +593.2840827
Tech Fax Ext:
Tech Email: DAVID@DDLINUX.COM
Name Server: DNS1.NAME-SERVICES.COM
Name Server: DNS2.NAME-SERVICES.COM
Name Server: DNS3.NAME-SERVICES.COM
Name Server: DNS4.NAME-SERVICES.COM
Name Server: DNS5.NAME-SERVICES.COM
DNSSEC: unSigned
Registrar Abuse Contact Email: abuse@enom.com
Registrar Abuse Contact Phone: +1.4252982646
URL of the ICANN WHOIS Data Problem Reporting System:
Last update of WHOIS database: 2015-03-23T11:14:48.00Z
Version 6.3 4/3/2002
```

FIGURA 3. 13: Información del dominio escenciaindigena.com.

Fuente: Extraída de http://www.chatox.com/whois/whois.php

El nivel de visibilidad en el canal “Redes de Datos” será la suma de todos los valores antes encontrados: P_V=20

b. Accesos

❖ Conocer solicitudes, servicios troyanos comunes que utilizan TCP para conexiones desde todas las direcciones y puertos sin filtrar que han enviado respuesta a un SYN TCP. La **FIGURA 3. 14** muestra que existen 6 puertos tcp. $\boldsymbol{P_A}$**=6**

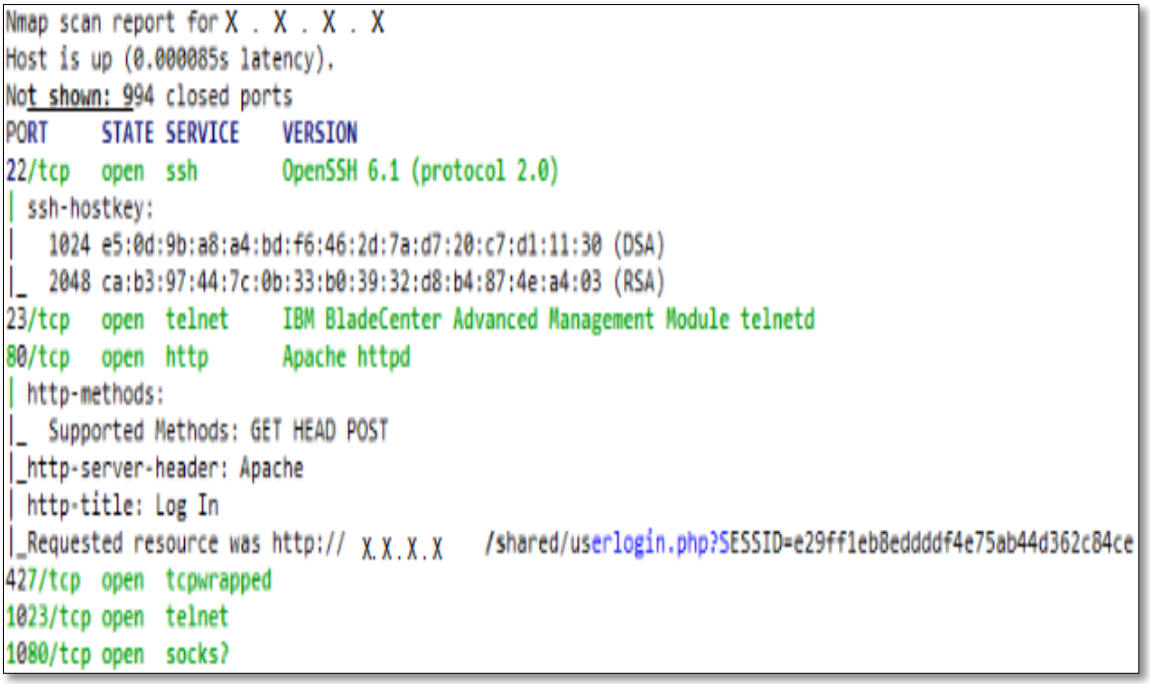


FIGURA 3. 14: SYN TCP.

Fuente: Obtenida del software Zenmap.

❖ Verificar los servicios de VoIP.

La cooperativa Escencia Indígena no cuenta con un sistema de VoIp. $\boldsymbol{P_A}$**=0**

❖ Relacionar cada puerto abierto a un demonio (servicio), aplicación (código específico o un producto que utiliza el servicio), y el protocolo (el medio para interactuar con ese servicio o aplicación).

En la **TABLA 3. 27** se puede observar los resultados de los escaneos realizados en la red de datos de la cooperativa Escencia Indígena, en donde se hace un análisis de algunos puertos y su relación con las aplicaciones y servicios. $\boldsymbol{P_A}$**=3**

TABLA 3. 27: Relación puertos y servicios.

Puerto			Análisis
5900	tcp	open	Es necesario que esté abierto para que el administrador pueda administrar el equipo mediante VNC.
80	tcp	open	Lo ideal sería bloquear sólo cierto tipo de tráfico desde el puerto 80; permitiendo la salida de datos.
443	tcp	open	Es lo correcto ya que es usado para la carga segura de páginas web.

Fuente: Desarrollo del proyecto en base a los resultados del software Zenmap.

- Verificar la disponibilidad del sistema operativo en comparación con las últimas vulnerabilidades y versiones de parches; tal como se observa en la **FIGURA 3. 15** $\boldsymbol{P_A}$=1

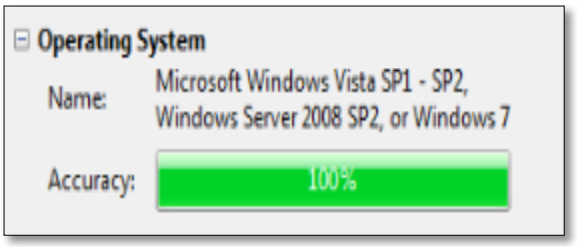


FIGURA 3. 15: Verificación de S.O

Fuente: Obtenida del software Zenmap.

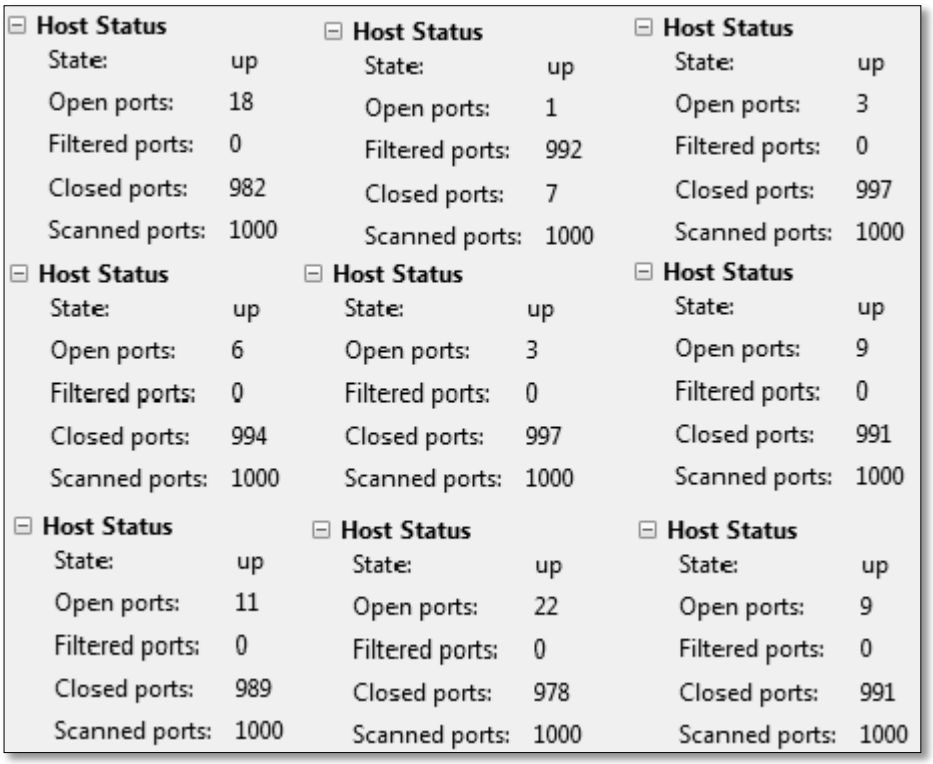
El nivel total de acceso en el canal de Redes de Datos será la suma de los valores mostrados anteriormente dando como resultado: P_A= 10

c. Confianza

Para una auditoría de seguridad de las redes de datos, el auditor cuenta cada tipo de servicio abierto o puerto abierto como una confianza (Herzog, 2003).

En la **FIGURA 3. 16** se puede observar los escaneos que se realizaron a diferentes servidores, en donde sumando todos los puertos abiertos se tiene:

El nivel de confianza en el canal “Red de Datos” igual a P_T= 82 el cual representa el número total de puertos abiertos.



Host Status	
State:	up
Open ports:	18
Filtered ports:	0
Closed ports:	982
Scanned ports:	1000

Host Status	
State:	up
Open ports:	1
Filtered ports:	992
Closed ports:	7
Scanned ports:	1000

Host Status	
State:	up
Open ports:	3
Filtered ports:	0
Closed ports:	997
Scanned ports:	1000

Host Status	
State:	up
Open ports:	6
Filtered ports:	0
Closed ports:	994
Scanned ports:	1000

Host Status	
State:	up
Open ports:	3
Filtered ports:	0
Closed ports:	997
Scanned ports:	1000

Host Status	
State:	up
Open ports:	9
Filtered ports:	0
Closed ports:	991
Scanned ports:	1000

Host Status	
State:	up
Open ports:	11
Filtered ports:	0
Closed ports:	989
Scanned ports:	1000

Host Status	
State:	up
Open ports:	22
Filtered ports:	0
Closed ports:	978
Scanned ports:	1000

Host Status	
State:	up
Open ports:	9
Filtered ports:	0
Closed ports:	991
Scanned ports:	1000

FIGURA 3. 16: Puertos abiertos en servidores.

Fuente: Elaborada en base a los resultados del software Zenmap.

3.4.2.2.2 CONTROLES

El siguiente paso en el cálculo de la RAV es definir los controles; los mecanismos de seguridad puestos en marcha para proteger las operaciones.

a. Autenticación

❖ Enumerar los accesos que requiere autenticación y documentar todos los privilegios descubiertos que se pueden utilizar para proporcionar acceso**.** $\boldsymbol{LC_{Au} = 1}$

Debido a que las aplicaciones requieren autenticación.

❖ Verificar el método de obtención de la autorización apropiada para la autenticación.

Proporcionada por el administrador de sistemas. $\boldsymbol{LC_{Au} = 1}$

❖ Verificar el método de ser identificados correctamente para contar la autenticación.

- Asignación de usuarios $\boldsymbol{LC_{Au} = 1}$

❖ Verificar la fortaleza de la autenticación a través de descifrado de contraseñas y volver a aplicar contraseñas a todos los puntos de acceso que requieren autenticación.

- Contraseñas robustas $\boldsymbol{LC_{Au} = 1}$

El nivel de autenticación en el canal “Red de Datos” es la suma de todos los factores considerados:

$$LC_{Au}=4$$

b. Indemnización

1. Documentar y enumerar los objetivos y servicios que están protegidos contra el abuso o la elusión de la política de los empleados, están asegurados por robo o daños, o utilizan de responsabilidad y de permisos renuncias.

2. Verificar la legalidad y la conveniencia de la lengua en los descargos de responsabilidad.

3. Verificar el efecto de las exenciones de responsabilidad sobre la seguridad o medidas de seguridad.

4. Examinar el lenguaje de la póliza de seguro para las limitaciones en los tipos de daños o activos.

El nivel de indemnización en el canal “Redes de Datos” es de:

$$LC_{Id}=4$$

Debido a que se consideró cuatro aspectos resultando el valor de uno en cada uno para indemnización.

c. Resistencia

La determinación y la medición de la resistencia de los objetivos en el ámbito de los cambios excesivos u hostiles diseñados para causar un fallo o degradación del servicio. Denegación de Servicio (DoS) es una situación en la que una circunstancia, ya sea intencional o accidentalmente, impide que el sistema funcione como está previsto. En ciertos casos, el sistema puede estar funcionando exactamente como se diseñó sin embargo, nunca fue pensado para manejar la carga, el alcance, o parámetros que se le impuso.

TABLA 3. 28: Resultados control Resistencia.

Resultados Control Resistencia
En este test se verificó que existen áreas del sistema que no están trabajando adecuadamente.

Fuente: Desarrollo del proyecto

El nivel de Resistencia en el canal “Redes de Datos” es: LC_{Re}=0

d. Subyugación

Enumerar y poner a prueba las insuficiencias de todos los canales a utilizar o permitir controles de pérdida no habilitados de forma predeterminada (Herzog, 2003).

De acuerdo al test realizado se ha encontrado que el nivel de subyugación es:

$$LC_{Su}=0$$

e. Continuidad

Enumerar y probar las deficiencias de todos los objetivos en materia de retrasos de acceso y los tiempos de respuesta de servicio a través de los sistemas de back-up.

Para dicho control se consideró los sistemas de back-up con los que se cuenta; en base a ello el control de continuidad es:

$$LC_{Ct}= 1$$

f. No Repudio

- Enumerar y probar para su uso o insuficiencias los sistemas de identificación y registro de acceso o las interacciones con la propiedad.

- Identificar métodos de identificación que la derrota repudio (Herzog, 2003).

El nivel de No Repudio para el canal “Redes de Datos” es:

$$LC_{NR}=0$$

g. Confidencialidad

- ❖ Enumerar todas las interacciones con los servicios en el ámbito de las comunicaciones o bienes transportados por el canal mediante líneas seguras, cifrado, interacciones para proteger la confidencialidad de la propiedad de la información entre las partes involucradas.

- ❖ Verificar los métodos aceptables utilizados para la confidencialidad.

- ❖ Prueba de la resistencia y el diseño del método de cifrado o la ofuscación.

- ❖ Verificar los límites exteriores de la comunicación que se pueden proteger a través de los métodos aplicados de confidencialidad (Herzog, 2003).

1. Cifrado de información para la comunicación con externos; lo cual añade un valor de 1 al control de confidencialidad en este canal.

$$LC_{Cf}=1$$

h. Privacidad

Relacionar información con los puertos TCP y UDP que no responden, para determinar si la disponibilidad depende de un tipo particular de contacto o protocolo (Herzog, 2003). En la **TABLA 3. 29** se puede observar el resumen de los puertos TCP y el respectivo análisis del estado del puerto.

TABLA 3. 29: Puertos y servicios bloqueados.

Puerto	Función del puerto	Análisis
22	Protocolo de transferencia de archivos.	Es importante que el puerto este cerrado para evitar la transferencia no autorizada de información.
23	Protocolo de acceso remoto sin seguridad.	El bloqueo es correcto ya que telnet no ofrece cifrado de claves.
113	Protocolo de identificación.	Sería importante mantenerlo abierto.
445	Servidor de dominio SMB de Microsoft.	El bloqueo es acertado ya que no es permitida la transferencia de archivos dentro de la red.

Fuente: Desarrollo del proyecto con resultados del software Zenmap.

Debido a que se tienen cuatros puertos bloqueados el control de privacidad en este canal es: LC_{Pr}=4

i. Integridad

En las redes de datos, el cifrado o un hash del archivo pueden proporcionar el control de integridad sobre el cambio del archivo en tránsito.

De acuerdo al test, el control de Integridad es: LC_{It}=1

Los datos son cifrados lo cual garantiza la integridad de los mismos.

j. Alarma

❖ En las redes de datos cuente cada servidor y el servicio en el que está basado, y si están monitoreados por el sistema de detección de intrusos.

- No se cuenta con un sistema de detección de intrusos

❖ Cuente cada servicio que mantiene un registro monitorizado de interacción.

- No se tiene un registro de monitoreo

❖ Cuentan los registros de acceso, incluso si no se utilizan para enviar una notificación de alerta de inmediato.

- No se mantiene un registro de acceso

El control de alarma en este canal es:

$$LC_{Al}=0$$

3.4.2.2.3 LIMITACIONES

El siguiente paso, es el cálculo de las limitaciones; las mismas que están consideradas individualmente. La ponderación de las vulnerabilidades, debilidades y preocupaciones se basan en una relación entre la suma OpSec, la pérdida de controles.

a. Vulnerabilidad

En la seguridad de los datos una vulnerabilidad puede ser un defecto en el software que permite a un atacante tener acceso para sobrescribir el espacio de memoria, una falla de cálculo que permite a un atacante bloquear el 100% del uso de la CPU o un sistema operativo que permite que los datos suficientes a se va a copiar en el disco hasta que no puede funcionar más (Herzog, 2003).

El tener sistemas operativos obsoletos representa vulnerabilidades, es por ello que de acuerdo al test, las vulnerabilidades en el canal de redes es:

$$L_V=6.$$

b. Debilidad

En la seguridad de los datos, una debilidad puede ser que permite intentos ilimitados de log-in a los servidores web (Herzog, 2003).

En la cooperativa Escencia Indígena se realiza un control de acceso a los servicios mediante la activación de dichos privilegios mediante la administración de usuarios y perfiles. Por este motivo el nivel de debilidad en este canal es:L_W=0

c. Preocupación

Cuente cada defecto o error en los controles del proceso: el no repudio, confidencialidad, privacidad, integridad y alarma (Herzog, 2003).

$$L_C= LC_{Cf}+LC_{Al}+LC_{It}+LC_{Pr}+LC_{NR}$$

$$L_C =1+0+1+4+0=6$$

d. Exposición

En la seguridad de los datos, una exposición puede ser una bandera descriptiva y válida acerca de un servicio o un ICMP echo reply desde un host (Herzog, 2003).

$$L_K=P_V \qquad L_K= 20$$

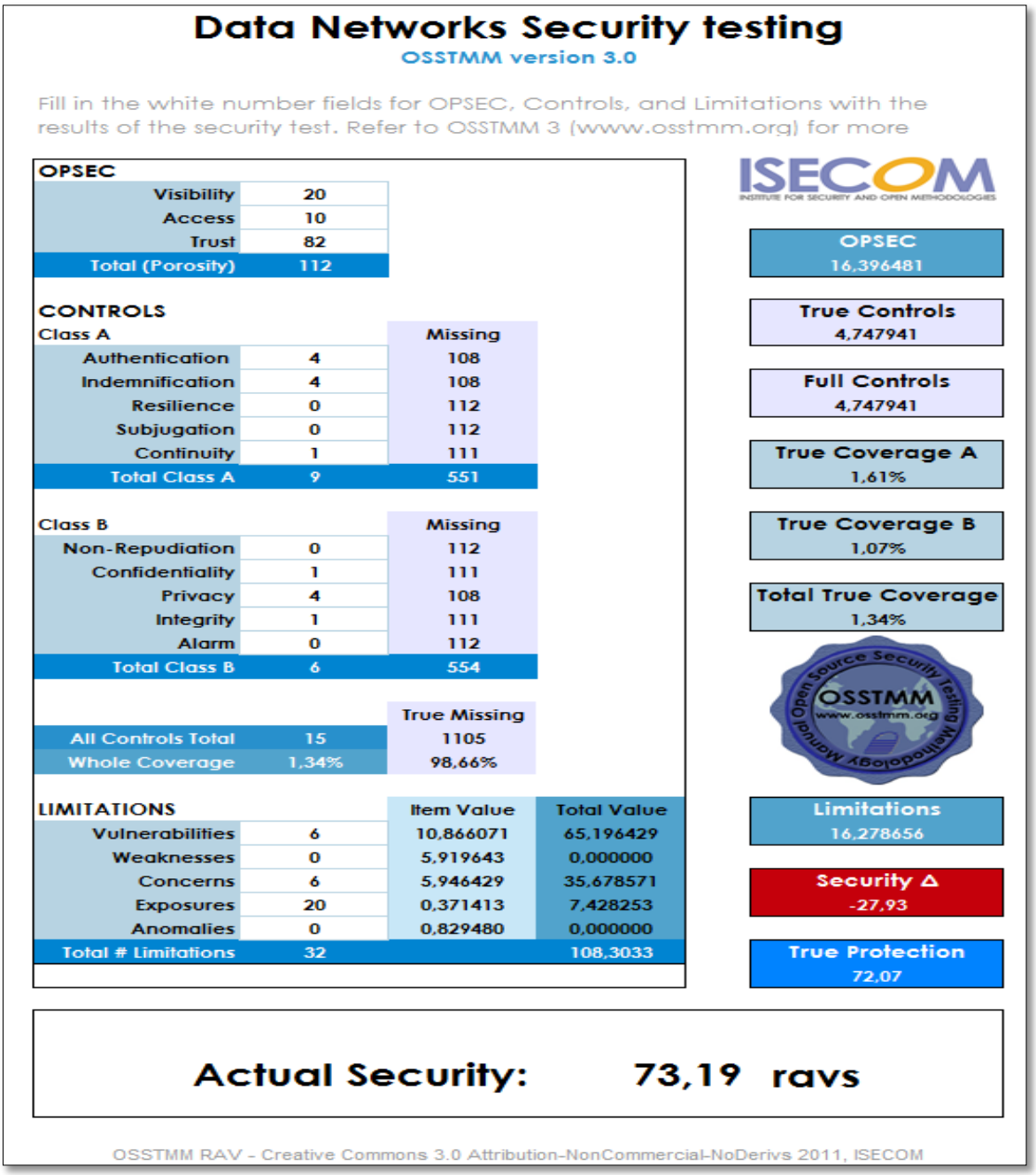
e. Anomalías

Cuente cada elemento identificable o desconocido que no puede tenerse en cuenta en las operaciones normales, por lo general cuando la fuente o el destino del elemento no se pueden entender. Una anomalía puede ser una señal temprana de un problema de seguridad. Dado que las incógnitas son los elementos que no pueden ser controlados, una auditoría adecuada requiere ir observando y anotando todas las anomalías (Herzog, 2003).

Durante el tiempo en que se realizó el test no se encontraron anomalías, por lo que:L_A=0

3.4.2.2.4 CÁLCULO DE RAVS

Una manera directa y más simple para hacer RAVs es usar las hojas de cálculo creadas específicamente calcular el área de ataque y varias métricas requeridas, populares a partir de los datos de prueba (Herzog, 2003). Los resultados se muestran en la **FIGURA 3. 17**



Data Networks Security testing

OSSTMM version 3.0

Fill in the white number fields for OPSEC, Controls, and Limitations with the results of the security test. Refer to OSSTMM 3 (www.osstmm.org) for more

OPSEC		
Visibility	20	
Access	10	
Trust	82	
Total (Porosity)	112	

CONTROLS		
Class A		Missing
Authentication	4	108
Indemnification	4	108
Resilience	0	112
Subjugation	0	112
Continuity	1	111
Total Class A	9	551
Class B		Missing
Non-Repudiation	0	112
Confidentiality	1	111
Privacy	4	108
Integrity	1	111
Alarm	0	112
Total Class B	6	554
		True Missing
All Controls Total	15	1105
Whole Coverage	1,34%	98,66%

LIMITATIONS		Item Value	Total Value
Vulnerabilities	6	10,866071	65,196429
Weaknesses	0	5,919643	0,000000
Concerns	6	5,946429	35,678571
Exposures	20	0,371413	7,428253
Anomalies	0	0,829480	0,000000
Total # Limitations	32		108,3033

OPSEC	16,396481
True Controls	4,747941
Full Controls	4,747941
True Coverage A	1,61%
True Coverage B	1,07%
Total True Coverage	1,34%
Limitations	16,278656
Security Δ	-27,93
True Protection	72,07

Actual Security: 73,19 ravs

OSSTMM RAV - Creative Commons 3.0 Attribution-NonCommercial-NoDerivs 2011, ISECOM

FIGURA 3. 17: Cálculo de RAVs canal Red de Datos.

Fuente: Obtenida de la Calculadora de RAVs de OSSTMM 3.0

3.4.2.2.5 INTERPRETACIÓN DE RESULTADOS

La seguridad operacional es muy alta, principalmente en el aspecto de confianza, en el que se ha considerado todos los puertos que están abiertos. Esto refleja la importancia que se le ha dado a la seguridad de las telecomunicaciones

De acuerdo al test realizado, se constató que se tienen únicamente controles de Indemnización, autenticación y privacidad; mientras tanto los demás controles son nulos; dando lugar a la inseguridad de la información.

Las limitaciones se valoran individualmente, pero éstas se relacionan directamente con algunos controles y seguridad operacional, por lo cual debido a que estos valores son muy altos hacen que el cálculo de las limitaciones también sea alto. Es así que resaltan limitaciones como las Vulnerabilidades, debilidades y exposiciones las mismas que reflejan una administración no adecuada que expone a la red a ciertas amenazas hacia la seguridad de información.

CAPÍTULO IV

4 DISEÑO DEL SISTEMA DE SEGURIDAD PERIMETRAL

En este capítulo se diseña el sistema de seguridad tanto a nivel de acceso como a nivel de distribución. A nivel de acceso se concientizará a los usuarios y administradores de los activos informáticos de la empresa mediante la creación de un manual de políticas de seguridad basado en los controles de la norma ISO/IEC 27002. A nivel de distribución se aplicará la norma para seleccionar adecuadamente el hardware y software que cumpla los requerimientos de la empresa.

4.1 POLÍTICAS DE SEGURIDAD

Una vez identificados los riegos de seguridad, se seleccionan controles que garanticen su reducción hasta un nivel aceptable; tomando en consideración que ningún conjunto de controles puede lograr la seguridad completa. Se propone crear una guía de políticas y buenas prácticas con el objetivo mejorar la gestión de la seguridad de la información, así como también concientizar a los funcionarios y administradores de los activos de información en el buen uso de los mismos.

Cooperativa de Ahorro y Crédito Escencia Indígena Ltda.		
ESCENCIA INDIGENA LTDA. COOPERATIVA DE AHORRO Y CRÉDITO	**Manual de Normas y Procedimientos de Seguridad de la Información**	
Versión:	1	
Revisado por:	Ing. Tarquino Morales Ing. Pablo Rivadeneira	
Aprobado por:	Ing. Serafín Maliza	
Fecha de aprobación:		

I. INTRODUCCIÓN

i. Seguridad de la información

La información constituye uno de los activos más importantes para una institución, independientemente de la forma en que se la almacene o transmita necesita protección contra la gran variedad de amenazas a las que se expone, todo con el fin de asegurar la continuidad, minimizar el riego y maximizar las oportunidades de crecimiento del negocio.

a. Alcance

La política incluye un conjunto apropiado de controles de gestión de la seguridad de la información en donde se concentra el procesamiento, almacenamiento y prestación de servicios.

b. Importancia

La importancia de implementar políticas que garanticen la seguridad de la información es mantener el correcto funcionamiento de las actividades de la empresa, cuidando la buena imagen, prestigio y reputación de la cooperativa Escencia Indígena.

ESCENCIA INDIGENA LTDA. COOPERATIVA DE AHORRO Y CRÉDITO	**Manual de Normas y Procedimientos de Seguridad de la Información**	

i. Marco referencial

a. Evaluación de riesgos

Los resultados del análisis de riesgos ayudan a proteger la información debido a que se encarga de identificar, clasificar y evaluar las amenazas y vulnerabilidades que perjudican la integridad y disponibilidad de la información.

b. Gestión del riesgo

El siguiente paso al análisis de riesgos es la aceptación de los mismos y la adecuada gestión que se aplique. Los controles a implementar se deben elegir de tal manera garantice las falencias encontradas.

Los controles se obtienen de la norma ISO/IEC 27002:2013, guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información.

ii. Políticas de seguridad

La política de seguridad es un medio de comunicación y soporte para la correcta administración de los activos de información. En ella se establece reglas y procedimientos que regulan la forma en que una organización previene, protege y maneja los riesgos de diferentes daños.

La política debe ser socializada al personal interno, socios, proveedores y terceros para una mejor funcionalidad.

II. OBJETIVO

Concientizar el uso adecuado de los activos informáticos y de los servicios que presta la Cooperativa de Ahorro y Crédito Escencia Indígena mediante un manual de políticas y buenas prácticas sobre la seguridad de la información.

ESCENCIA INDIGENA LTDA. COOPERATIVA DE AHORRO Y CRÉDITO	**Manual de Normas y Procedimientos de Seguridad de la Información**	

III. RESPONSABILIDADES

Es responsabilidad de la autoridad del departamento de sistemas desarrollar, mantener y mejorar la gestión de la seguridad de la información en la institución; así como también de capacitar a todos los funcionarios sobre las políticas y procedimientos en la jornada laboral.

Todos los funcionarios de la institución tienen las siguientes responsabilidades:

- Respetar sus roles y funciones sin abusar de los privilegios de acceso que se le asigne, actuar siempre con ética y moral.
- Conocer la política de seguridad de la información y aplicarla en sus funciones diarias.
- Reportar los incidentes de seguridad detectados a lo largo de la jornada laboral a los miembros responsables de la seguridad de la información.

IV. VIGENCIA

El manual de normas y procedimientos entrará en vigencia una vez aprobado por las autoridades pertinentes de la cooperativa. Puede ser actualizado o modificado conforme sucedan los eventos de seguridad o por implementación de nuevos equipos, servicios o sistemas, siempre que se cumplan los objetivos de la seguridad y de la empresa.

ESCENCIA INDIGENA LTDA. COOPERATIVA DE AHORRO Y CRÉDITO	**Manual de Normas y Procedimientos de Seguridad de la Información**	

I. MARCO NORMATIVO

El presente documento se realizó en base a la Norma NTE INEN-ISO/IEC 27002:3013; la misma que establece directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización. Los objetivos indicados en esta norma brindan una guía general sobre las metas aceptadas comúnmente para la gestión de la seguridad de la información.

Es importante recordar que ningún conjunto de controles puede lograr la seguridad completa y que se deben implementar acciones adicionales para mejorar la eficiencia y la eficacia de la seguridad de la información.

II. ESTRUCTURA

Este documento está estructurado en base a los siguientes dominios y controles que se tomados de la Norma NTE INEN-ISO/IEC 27002:2013.

1. Políticas de la seguridad

1.1. Directrices de la dirección en seguridad de la información.

1.1.1. Conjunto de políticas para la seguridad de la información.

1.1.2. Revisión de la política de la seguridad de la información.

2. Aspectos organizativos de la seguridad de la información

2.1. Organización interna

2.1.1. Asignación de responsabilidades para la seguridad de la información.

2.2. Dispositivos para la movilidad y teletrabajo

2.2.1. Políticas de uso de dispositivos para movilidad

2.2.2. Teletrabajo

ESCENCIA INDIGENA LTDA. COOPERATIVA DE AHORRO Y CRÉDITO	**Manual de Normas y Procedimientos de Seguridad de la Información**	

8. Seguridad en la operativa

8.1. Responsabilidades y procedimientos de operación

8.1.1. Documentación de procedimientos de operación

8.2. Protección contra el código malicioso

8.2.1. Controles contra códigos maliciosos

8.3. Copias de seguridad

8.3.1. Copias de seguridad de la información

8.4. Control del software en explotación

8.4.1. Instalación del software en sistemas en producción

8.5. Gestión de la vulnerabilidad técnica

8.5.1. Gestión de las vulnerabilidades técnicas

8.5.2. Restricciones en la instalación de software

9. Seguridad en las telecomunicaciones

9.1. Gestión de la seguridad en las redes

9.1.1. Mecanismos de seguridad asociados a servicios en red

9.2. Intercambio de información con partes externas

92.1 Políticas y procedimientos de intercambio de información

10. Adquisición, desarrollo y mantenimiento de los sistemas de información

10.1. Requisitos de seguridad de los sistemas de información

10.1.1. Análisis y especificación de los requisitos de seguridad

10.2. Seguridad en los procesos de desarrollo y soporte

10.2.1. Restricciones a los cambios en los paquetes de software

10.3. Datos de prueba

10.3.1. Protección de los datos utilizados en pruebas

14.2.1. Cumplimiento de las políticas y normas de seguridad

III. TÉRMINOS Y DEFINICIONES

Para el propósito de este documento se aplican los siguientes términos y definiciones.

Activo	Es un componente o una parte de un sistema global al que la organización asigna un valor y, por tanto, que requiere protección.
Amenaza	Es un peligro posible que podría explotar una vulnerabilidad.
Ataque	Es un asalto a la seguridad del sistema derivado de una amenaza inteligente; es decir, un acto inteligente y deliberado para eludir los servicios de seguridad y violar la política de seguridad de un sistema.
Autenticidad	Garantiza que un usuario es quien dice ser mediante su autenticación y registro.
Confiabilidad	Es el grado de garantías en que las prácticas se han realizado tal y como se tenía planeados.
Confidencialidad	Protección de la información ante accesos no autorizados.
Control	Medios para gestionar el riesgo, incluyendo políticas, procedimientos, prácticas o estructuras.
Disponibilidad	Se refiere a que todos los elementos que componen el sistema puedan recuperarse rápida y completamente ante una interrupción inesperada.
Gusanos	Son programas que realizan copias de sí mismos, alojándolas en diferentes ubicaciones del computador
Hardware	Son todos los componentes físicos, es decir, todo lo que se puede ver y palpar.

IEC	Comisión Electrotécnica Internacional; participa en el desarrollo de las Normas Internacionales.
Integridad	Enfocada a la exactitud de los datos; se los protege de alteraciones no autorizadas, no controladas u ocasionadas accidentalmente no solo en su trayecto sino también en el origen.
Interceptación	Se refiere interrumpir una vía de comunicación para apoderarse de algo antes que llegue al destino.
ISO	Organización Internacional para la Estandarización, que regula una serie de normas para fabricación, comercio y comunicación, en todas las ramas industriales.
No repudio	Proporciona protección contra la interrupción por parte de una de las entidades implicadas en la comunicación, de haber participado en toda o parte de la comunicación
Responsabilidad	Es el requisito que permite que pueda trazarse las acciones de una entidad de forma única.
Seguridad de la información	Prevención de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no-repudio y confiabilidad pueden estar involucradas.
Software	Son todos los programas y/o aplicaciones que permiten realizar tareas específicas; no existen físicamente, es decir, no se pueden ver ni palpar.

Software antivirus	Es un programa que detecta, previene y toma medidas para eliminar programas de software malintencionados, como virus y gusanos.
UPS	Dispositivo que proporciona energía temporal cuando se dé un corte de energía en el suministro de la red eléctrica.
Usuario	Es aquella persona que utiliza los recursos del sistema de información y/o comunicación.
Virus	Son pequeños programas diseñados para propagarse de una computadora a otra e interferir con el funcionamiento de las mismas. Estos pueden propagarse a menudo a través de documentos adjuntos en mensajes de correo electrónico y en las descargas de internet.
Vulnerabilidad	Es un punto débil que por sí mismo no causa ningún daño, pero al ser explotado por amenazas afectan la confidencialidad, disponibilidad e integridad de la información de una persona o una empresa

ESCENCIA INDIGENA LTDA. COOPERATIVA DE AHORRO Y CRÉDITO	**Manual de Normas y Procedimientos de Seguridad de la Información**	

I. DESARROLLO DE LAS POLÍTICAS DE SEGURIDAD

Dominio	1. Políticas de la seguridad	**Destinatario**
Objetivos de Control	1.1 Directrices de la dirección en seguridad de la información	Equipo de trabajo del departamento de sistemas
Control	1.1.1 Conjunto de políticas para la seguridad de la información	

Art. 1. La Coordinación de sistemas elaborará un Manual de Políticas de Seguridad de la Información, en el que se explique el cumplimiento de los requisitos legales y reglamentos, así como también, los requisitos de educación, formación y concienciación sobre seguridad y las consecuencias de las violaciones de dichas políticas.

Art. 2. El Manual de Políticas de Seguridad de la Información se deberá comunicar de manera pertinente, accesible y compresible a todos los funcionarios de la institución.

Dominio	1. Políticas de la seguridad	**Destinatario**
Objetivos de Control	1.1 Directrices de la dirección en seguridad de la información.	Equipo de trabajo del departamento de sistemas
Control	1.1.2 Revisión de la política de la seguridad de la información.	

Art.3. La Coordinación de sistemas deberá asumir la responsabilidad de la revisión periódica de los lineamientos y del Manual de Políticas de Seguridad de la Información, para garantizar que éste siga siendo adecuado, suficiente y eficaz.

Art.4. Se definirán procedimientos programados para la revisión del Manual de Políticas de Seguridad de la Información, además se tomará en cuenta cambios significativos que pudieran afectar el entorno de la organización, incidentes reportados por los usuarios, recomendaciones de las autoridades y tendencias relacionadas con amenazas y vulnerabilidades.

ESCENCIA INDIGENA LTDA. COOPERATIVA DE AHORRO Y CRÉDITO	**Manual de Normas y Procedimientos de Seguridad de la Información**	

Dominio	2. Aspectos organizativos de la seguridad de la información	**Destinatario**
Objetivos de Control	2.1 Organización interna	Equipo de trabajo del departamento de sistemas
Control	2.1.1 Asignación de responsabilidades para la seguridad de la información.	

Art. 5. La Coordinación de sistemas deberá definir las responsabilidades de protección de los activos y procesos de seguridad individuales para ejecutar procesos específicos de seguridad.

Art. 6. De ser necesario aquellos individuos responsables de la seguridad, pueden delegar las labores a otros. Sin embargo siguen siendo responsables y deben asegurarse de la correcta ejecución de las labores delegadas.

Dominio	2. Aspectos organizativos de la seguridad de la información	**Destinatario**
Objetivos de Control	2.2 Dispositivos para la movilidad y teletrabajo	Equipo de trabajo del departamento de sistemas
Control	2.2.1 Políticas de uso de dispositivos para movilidad	

Art. 7. El uso de los equipos portátiles fuera de las instalaciones de la cooperativa, únicamente se permitirá a usuarios autorizados por la Dirección del departamento de sistemas, previa solicitud de la dependencia respectiva.

ESCENCIA INDIGENA LTDA. COOPERATIVA DE AHORRO Y CRÉDITO	**Manual de Normas y Procedimientos de Seguridad de la Información**	

Dominio	2. Aspectos organizativos de la seguridad de la información	**Destinatario**
Objetivos de Control	2.2. Dispositivos para la movilidad y teletrabajo	Equipo de trabajo del departamento de sistemas
Control	2.2.2 Teletrabajo	

Art. 8. Cualquier funcionario de la cooperativa, autorizado por la dirección de sistemas, que requiera tener acceso a la información de la Institución desde redes externas, podrá acceder remotamente mediante un proceso de autenticación; uso de conexiones seguras.

Art. 9. Se determinarán diferentes medios de control utilizados para identificar, verificar y confirmar la autenticidad de la persona u organización externa que se vaya involucrar de manera directa con los activos de la institución.

Dominio	3. Seguridad ligada a los recursos humanos	**Destinatario**
Objetivos de Control	3.1 Antes de la contratación	Equipo de trabajo del departamento de sistemas
Control	3.1.1 Investigación de antecedentes	

Art. 10. El coordinador de Recursos Humanos tendrá que verificar los antecedentes judiciales, disciplinarios y seguimiento a la hoja de vida de todos los candidatos a emplear de conformidad con el reglamento interno de la institución.

ESCENCIA INDIGENA LTDA. COOPERATIVA DE AHORRO Y CRÉDITO	**Manual de Normas y Procedimientos de Seguridad de la Información**	

Dominio	3. Seguridad ligada a los recursos humanos	**Destinatario**
Objetivos de Control	3.1 Antes de la contratación	Equipo de trabajo del departamento de sistemas
Control	3.1.2 Términos y condiciones de contratación	

Art. 11. Los acuerdos contractuales con los empleados y los contratistas deberán establecer las responsabilidades establecidas por la cooperativa en el cumplimiento de la presente Política de Seguridad de la Información.

Dominio	3. Seguridad ligada a los recursos humanos	**Destinatario**
Objetivos de Control	3.2 Durante la contratación	Equipo de trabajo del departamento de sistemas
Control	3.2.1 Responsabilidades de gestión	

Art. 12. La administración pedirá a todos los empleados y contratistas, aplicar la seguridad de la información de acuerdo con las políticas y procedimientos establecidos. Todos los empleados y/contratistas tendrán acceso permanente a la política y se obligan a cumplirla.

Art. 13. El personal que ingrese de manera temporal y/o indefinida a la institución, deberá firmar que conoce y acepta lo definido en la política de Seguridad de manera obligatoria.

ESCENCIA INDIGENA LTDA. COOPERATIVA DE AHORRO Y CRÉDITO	**Manual de Normas y Procedimientos de Seguridad de la Información**	

Dominio	3. Seguridad ligada a los recursos humanos	**Destinatario**
Objetivos de Control	3.2 Durante la contratación	Equipo de trabajo del departamento de sistemas
Control	3.2.2 Concienciación, educación y capacitación en seguridad de la información	

Art. 14. La Dirección Técnica de Información y Tecnología realizará capacitaciones a todos los empleados y contratistas de la organización de sensibilización, educación y formación adecuada y actualizaciones periódicas en las políticas y procedimientos de la organización, que sea relevante para su función laboral.

Art. 15. Será responsabilidad de cada usuario solicitar capacitación al personal del departamento de sistemas en el manejo de paquetes informáticos utilizados en los equipos, con el fin de evitar fallas que pongan en riesgo la seguridad de la información.

Dominio	3. Seguridad ligada a los recursos humanos	**Destinatario**
Objetivos de Control	3.2 Durante la contratación	Equipo de trabajo del departamento de sistemas
Control	3.2.3 Proceso disciplinario	

Art. 16. Se solicitará proceso disciplinario formal y comunicado en lugar de tomar medidas contra los empleados que hayan cometido una violación de la seguridad de la información.

ESCENCIA INDIGENA LTDA. COOPERATIVA DE AHORRO Y CRÉDITO	**Manual de Normas y Procedimientos de Seguridad de la Información**	

Dominio	3. Seguridad ligada a los recursos humanos	**Destinatario**
Objetivos de Control	3.3 Cese o cambio de puesto de trabajo	Equipo de trabajo del departamento de sistemas
Control	3.3.1 Cese o cambio de puesto de trabajo	

Art. 17. Es obligación de los funcionarios de la cooperativa definir y hacer cumplir las responsabilidades de seguridad de la información y tareas que siguen vigentes después de la terminación o cambio de puesto de trabajo.

Art. 18. Una vez culminado el contrato de trabajo todos los empleados, contratistas o usuarios de terceras partes están en la obligación de devolver todos los activos pertenecientes a la institución que se encuentren en su poder.

Dominio	4. Gestión de activos	**Destinatario**
Objetivos de Control	4.1 Responsabilidad por los activos	Equipo de trabajo del departamento de sistemas
Control	4.1.1 Inventario de activos	

Art. 19. Se deberá identificar todos los activos informáticos y relacionados con la seguridad de la información; documentando toda la información necesaria que indique su tipo, ubicación, estado, etc.; obteniendo así el inventario de los equipos tecnológicos de la cooperativa.

ESCENCIA INDIGENA LTDA. COOPERATIVA DE AHORRO Y CRÉDITO	**Manual de Normas y Procedimientos de Seguridad de la Información**	

Dominio	4. Gestión de activos	**Destinatario**
Objetivos de Control	4.1 Responsabilidad por los activos	Equipo de trabajo del departamento de sistemas
Control	4.1.2 Devolución de activos	

Art. 20. Todos los empleados, contratistas o usuarios de terceras partes deberán devolver todos los activos pertenecientes a la institución que se encuentren en su poder al finalizar su contratación laboral.

Art. 21. Si un empleado, contratista o usuario de terceras partes utiliza su propio equipo, se deberá garantizar que toda la información sea transferida a la cooperativa y se elimine en su totalidad de tal equipo, si se ha finalizado su contratación laboral.

Dominio	4. Gestión de activos	**Destinatario**
Objetivos de Control	4.2 Clasificación de la información	Equipo de trabajo del departamento de sistemas
Control	4.2.1 Etiquetado y manipulado de la información	

Art. 22. La información y los equipos informáticos deberán ser clasificados y etiquetados dependiendo de su valor relativo, privacidad, sensibilidad, el nivel de riesgo a que está expuesta y/o requerimientos legales de retención.

ESCENCIA INDIGENA LTDA. COOPERATIVA DE AHORRO Y CRÉDITO	**Manual de Normas y Procedimientos de Seguridad de la Información**	

Dominio	5. Control del acceso	**Destinatario**
Objetivos de Control	5.1 Requisitos de negocio para el control de accesos	Equipo de trabajo del departamento de sistemas
Control	5.1.1 Política de control de accesos	

Art. 23. Se deberá garantizar entornos con controles de acceso idóneos, los cuales aseguran el perímetro, tanto en oficinas, recintos, áreas de carga y descarga, así como en entornos abiertos para evitar el acceso no autorizado a ellos.

Art. 24. El acceso a áreas seguras donde se procesa o almacena información confidencial y restringida, es limitado únicamente a personas autorizadas.

Art. 25. El acceso a áreas seguras debe requerir esquemas de control de acceso, como tarjetas, llaves o candados.

Art. 26. Se restringe el acceso físico a dispositivos como: puntos de acceso inalámbricos, puertas de enlace a redes y terminales de red que estén ubicadas en las áreas seguras.

Dominio	5. Control de acceso	**Destinatario**
Objetivos de Control	5.1 Requisitos de negocio para el control de accesos	Equipo de trabajo del departamento de sistemas
Control	5.1.2 Control de acceso a las redes y servicios asociados	

Art. 27. Los usuarios que dispongan de acceso y servicios de la red son los que han sido específicamente autorizados para su uso.

Art. 28. Cada usuario es responsable por sus acciones mientras usa cualquier recurso de Información de la empresa.

ESCENCIA INDIGENA LTDA. COOPERATIVA DE AHORRO Y CRÉDITO	**Manual de Normas y Procedimientos de Seguridad de la Información**	

Dominio	5. Control del acceso	**Destinatario**
Objetivos de Control	5.1 Requisitos de negocio para el control de accesos	Equipo de trabajo del departamento de sistemas
Control	5.1.2 Control de acceso a las redes y servicios asociados	

Art. 29. Los niveles de acceso deben reflejar permanentemente una necesidad clara y demostrada de negocio y no deben comprometer la segregación de funciones y responsabilidades.

Dominio	5. Control de acceso	**Destinatario**
Objetivos de Control	5.2 Gestión de acceso de usuario	Equipo de trabajo del departamento de sistemas
Control	5.2.1 Gestión de altas/bajas en el registro de usuarios	

Art. 30. Todos los funcionarios de la red de la institución deberán contar con una identificación de usuario (ID), con la que se vinculará y se responsabilizará de sus acciones con el uso de sistemas o servicios de información.

Art. 31. La eliminación de un identificador de usuario debe ser realizada inmediatamente haya finalizado su relación contractual del usuario con la institución.

Art. 32. La coordinación de sistemas deberá emitir a todos los usuarios una declaración escrita de sus derechos de acceso; misma que será firmada por los funcionarios indicando que entienden y aceptan las condiciones establecidas.

ESCENCIA INDIGENA LTDA. COOPERATIVA DE AHORRO Y CRÉDITO	**Manual de Normas y Procedimientos de Seguridad de la Información**	

Dominio	5. Control del acceso	**Destinatario**
Objetivos de Control	5.2 Gestión de acceso de usuario	Equipo de trabajo del departamento de sistemas
Control	5.2.2 Gestión de los derechos de acceso asignados a usuarios	

Art. 33. El acceso a la información de la institución es otorgado sólo a usuarios autorizados, basados en los requerimientos para cumplir con las tareas relacionadas con su responsabilidad o tipo de servicio.

Art. 34. Los eventos de ingreso y autenticación de usuarios serán registrados y monitoreados por los responsables de la información.

Dominio	5. Control de acceso	**Destinatario**
Objetivos de Control	5.2 Gestión de acceso de usuario	Equipo de trabajo del departamento de sistemas
Control	5.2.3 Gestión de los derechos de acceso con privilegios especiales	

Art. 35. Se deberá restringir y controlar el uso de las claves de usuarios administradoras, tales como: “root”, “adm” y “system”, entre otros, deben ser controladas acorde como lo establece los lineamientos que hacen parte de esta política.

ESCENCIA INDIGENA LTDA. COOPERATIVA DE AHORRO Y CRÉDITO	**Manual de Normas y Procedimientos de Seguridad de la Información**	

Dominio	5. Control del acceso	**Destinatario**
Objetivos de Control	5.3 Responsabilidades del usuario	Equipo de trabajo del departamento de sistemas
Control	5.3.1 Uso de información confidencial para la autenticación	

Art. 36. El personal de trabajo de la Coordinación de sistemas emitirá una charla de las buenas prácticas de la seguridad en la selección y el uso adecuado de las contraseñas.

Art. 37. Evitar conservar registros de las contraseñas en papeles o archivos que estén a la vista de cualquier usuario.

Art. 38. Es responsabilidad de cada usuario cambiar periódicamente su contraseña, evitando reutilizar contraseñas antiguas. En caso de no saber hacerlo pedir asesoría al personal del departamento de sistemas de la institución.

Dominio	5. Control de acceso	**Destinatario**
Objetivos de Control	5.4 Control de acceso a sistemas y aplicaciones	Equipo de trabajo del departamento de sistemas
Control	5.4.1 Restricción del acceso a la información	

Art. 39. El acceso a la información de la institución será restringido y limitado únicamente para los funcionarios que realmente la requiera en función de sus labores.

ESCENCIA INDIGENA LTDA. COOPERATIVA DE AHORRO Y CRÉDITO	**Manual de Normas y Procedimientos de Seguridad de la Información**	

Dominio	5. Control del acceso	**Destinatario**
Objetivos de Control	5.4 Control de acceso a sistemas y aplicaciones	Equipo de trabajo del departamento de sistemas
Control	5.4.2 Gestión de contraseñas de usuario	

Art. 40. Se establecerá una contraseña temporal a todos los usuarios para el ingreso a sistemas, la misma que deberá ser cambiada inmediatamente por cada usuario.

Art. 41. La longitud mínima en una contraseña se establece en 8 caracteres y un máximo de 15; sean estos alfanuméricos y especiales; de preferencia que contenga una letra mayúscula, un alfanumérico, un especial.

Art. 42. La contraseña deberá ser única y no descifrable es decir no utilizar palabras muy comunes.

Dominio	5. Control de acceso	**Destinatario**
Objetivos de Control	5.4 Control de acceso a sistemas y aplicaciones	Equipo de trabajo del departamento de sistemas
Control	5.4.3 Uso de herramientas de administración de sistemas	

Art. 43. Se restringe el uso de programas de utilidad que atenten contra el buen funcionamiento del sistema y de aplicaciones de la empresa.

ESCENCIA INDIGENA LTDA. COOPERATIVA DE AHORRO Y CRÉDITO	**Manual de Normas y Procedimientos de Seguridad de la Información**	

Dominio	6. Cifrado	**Destinatario**
Objetivos de Control	6.1 Controles criptográficos	Equipo de trabajo del departamento de sistemas
Control	6.1.1 Política de uso de los controles criptográficos	

Art. 44. Las claves de acceso a sistemas, datos y servicios deberán ser encriptados.

Art. 45. Se deberá encriptar la transmisión de información con destino externo a la institución.

Art. 46. Se encriptará también el resguardo de la información obtenida en una evaluación de riegos informáticos.

Dominio	6. Cifrado	**Destinatario**
Objetivos de Control	6.1 Controles criptográficos	Equipo de trabajo del departamento de sistemas
Control	6.1.2 Gestión de claves	

Art. 47. Se deberán establecer métodos criptográficos que generen claves que tengan protección contra modificación, pérdida, destrucción y divulgación no autorizada.

Art. 48. Se deberá contar con un sistema de gestión de claves basado en un conjunto de normas, procedimientos y métodos seguros para:

- Generar y obtener certificados de claves públicas
- Cambiar o actualizar las claves incluyendo reglas de cuando y como cambiarlas.
- Recuperar claves pérdidas como parte de la gestión de continuidad del negocio.

ESCENCIA INDIGENA LTDA. COOPERATIVA DE AHORRO Y CRÉDITO	**Manual de Normas y Procedimientos de Seguridad de la Información**	

Dominio	7. Seguridad física y ambiental	**Destinatario**
Objetivos de Control	7.1 Áreas seguras	Equipo de trabajo del departamento de sistemas
Control	7.1.1 Perímetro de seguridad física	

Art. 49. Se establecerán los perímetros de la seguridad y la ubicación de cada lugar que contenga servicios de procesamiento de información y protegerlos con paredes externas, puertas con protección adecuada contra el acceso no autorizado con medidas de control tales como barras, alarmas, relojes, biométricos, etc.

Art. 50. Se deberá establecer un área de recepción con personal u otro medio para controlar el acceso físico a los sitios con acceso restringido.

Dominio	7. Seguridad física y ambiental	**Destinatario**
Objetivos de Control	7.1 Áreas seguras	Equipo de trabajo del departamento de sistemas
Control	7.1.2 Controles físicos de entrada	

Art. 51. El ingreso al cuarto de equipos de la institución será, única y exclusivamente al personal del departamento de sistemas.

Art. 52. Al personal de servicio de mantenimiento y/o soporte de terceras partes se le deberá dar acceso restringido al cuarto de equipos; es decir éste será autorizado previamente por el jefe del departamento de sistemas y será supervisado por el mismo.

Dominio	7. Seguridad física y ambiental	**Destinatario**
Objetivos de Control	7.1 Áreas seguras	Equipo de trabajo del departamento de sistemas
Control	7.1.3 Seguridad de oficinas, despachos y recursos	

Art. 53. No se deberá tener indicaciones, o señales visibles que identifiquen la presencia de actividades de procesamiento de información.

Art. 54. Se deberá rediseñar y/o reubicar las oficinas y recintos de procesamiento de información, evitando el acceso al público a los mismos y considerando para ello los reglamentos y las normas pertinentes de seguridad y salud.

Dominio	7. Seguridad física y ambiental	**Destinatario**
Objetivos de Control	7.1 Áreas seguras	Equipo de trabajo del departamento de sistemas
Control	7.1.4 Protección contra amenazas externas y ambientales.	

Art. 55. El cuarto de equipo deberá contar con protecciones físicas contra daños por incendio, inundación, terremoto, explosión, manifestaciones sociales y otras formas de desastre natural o artificial.

ESCENCIA INDIGENA LTDA. COOPERATIVA DE AHORRO Y CRÉDITO	**Manual de Normas y Procedimientos de Seguridad de la Información**	

Dominio	7. Seguridad física y ambiental	**Destinatario**
Objetivos de Control	7.2 Seguridad de los equipos	Equipo de trabajo del departamento de sistemas
Control	7.2.1 Emplazamiento y protección de los equipos	

Art. 56. Los equipos inherentes al procesamiento de la información deberán ser ubicados y protegidos contra amenazas ambientales y reducir la oportunidad de acceso no autorizado.

Art. 57. La selección del lugar de los activos de información permitirá otorgar un control visual y supervisión en todo momento. De necesario se deberá separar los activos de información de suma importancia a lugares mucho más seguros y establecer el nivel de seguridad requerida.

Art. 58. Se deberá aplicar mecanismos de protección contra variaciones de voltaje, fallos eléctricos, interrupciones de energía que afecten la disponibilidad y continuidad del negocio.

Art.59. Se prohíbe el consumo de alimentos y bebidas mientras se esté manipulando los equipos informáticos, debido a que puede ocasionar daños al equipo.

Dominio	7. Seguridad física y ambiental	**Destinatario**
Objetivos de Control	7.2 Seguridad de los equipos	Equipo de trabajo del departamento de sistemas
Control	7.2.2 Seguridad del cableado	

Art. 60. El cableado de energía y comunicaciones estarán protegidos contra interceptaciones o daños, ubicándolos en zonas no disponibles al público mediante la utilización de conductos o canaletas, separar líneas de energía eléctrica del cable de datos evitando interferencias.

Dominio	7. Seguridad física y ambiental	**Destinatario**
Objetivos de Control	7.2 Seguridad de los equipos	Equipo de trabajo del departamento de sistemas
Control	7.2.3 Mantenimiento de los equipos	

Art. 61. Todas las estaciones de trabajo que requieran mantenimiento por fallos en el hardware y/o software deberán ser reparados únicamente por los miembros del departamento de sistemas.

Art. 62. El personal del departamento de sistemas deberá realizar un informe que contenga las fallas encontradas y de todo el mantenimiento preventivo y correctivo.

Art. 63. Se deberá especificar un calendario para realizar mantenimiento preventivo de las estaciones de trabajo de la institución.

Dominio	7 .Seguridad física y ambiental	**Destinatario**
Objetivos de Control	7.2 Seguridad de los equipos	Equipo de trabajo del departamento de sistemas
Control	7.2.4 Salida de activos fuera de las dependencias de la empresa	

Art. 64. Cualquier equipo de procesamiento de la información no debe salir de las instalaciones de la institución a menos que sea autorizado por el responsable del departamento de sistemas y autoridad pertinente.

Art. 65. El funcionario que solicite la salida del activo fuera de las instalaciones de la empresa se hace responsable del cuidado de la integridad del mismo.

Dominio	7. Seguridad física y ambiental	**Destinatario**
Objetivos de Control	7.2 Seguridad de los equipos	Equipo de trabajo del departamento de sistemas
Control	7.2.5 Política de puesto de trabajo despejado y bloqueo de pantalla	

Art. 66. Los puestos de trabajo deben estar limpios de papeles, soportes de almacenamiento extraíbles y cuando se tenga que ausentar se recomienda el uso de llaves físicas, contraseñas, bloqueo de pantalla u otro tipo de control.

Art. 67. Los dispositivos de almacenamiento no utilizados deberán incorporar por un proceso de borrado o sobre escritura de los datos a fin de evitar fuga o sustracción información por personas no autorizadas.

Art. 68. Las fotocopiadoras deben estar protegidas del uso no autorizado mediante códigos de seguridad.

Dominio	8. Seguridad en la operativa	**Destinatario**
Objetivos de Control	8.1 Responsabilidades y procedimientos de operación	Equipo de trabajo del departamento de sistemas
Control	8.1.1 Documentación de procedimientos de operación	

Art. 68. Los procedimientos de operación deberán ser documentados y puestos a disposición de los usuarios que los necesiten.

ESCENCIA INDIGENA LTDA. COOPERATIVA DE AHORRO Y CRÉDITO	**Manual de Normas y Procedimientos de Seguridad de la Información**	

Dominio	8. Seguridad en la operativa	**Destinatario**
Objetivos de Control	8.1 Responsabilidades y procedimientos de operación	Equipo de trabajo del departamento de sistemas
Control	8.1.1 Documentación de procedimientos de operación	

Art. 69. Se deberá elaborar manuales de configuración y operación de los sistemas operativos, servicios de red, bases de datos y sistemas de información, así como todos los componentes de la plataforma tecnológica de la empresa; los mismos que deben estar documentados y disponibles para los usuarios que los requieran.

Art. 70. Se debe garantizar la documentación y actualización de los procedimientos relacionados con la operación y administración de la plataforma tecnológica que apoya los procesos de negocio de la cooperativa.

Dominio	8. Seguridad en la operativa	**Destinatario**
Objetivos de Control	8.2 Protección contra el código malicioso	Equipo de trabajo del departamento de sistemas
Control	8.2.1 Controles contra códigos maliciosos	

Art. 71. Se recomienda no descargar, adquirir o utilizar software cuya fuente no es reconocida como una fuente confiable.

Art. 72. Todas las estaciones de trabajos, servidores y demás equipos informáticos deberán tener instalado software antivirus activo con sus respectivas actualizaciones.

ESCENCIA INDIGENA LTDA. COOPERATIVA DE AHORRO Y CRÉDITO	**Manual de Normas y Procedimientos de Seguridad de la Información**	

Dominio	8. Seguridad en la operativa	**Destinatario**
Objetivos de Control	8.3 Copias de seguridad	Equipo de trabajo del departamento de sistemas
Control	8.3.1 Copias de seguridad de la información	

Art. 69. El responsable de software dentro del departamento de sistemas, realizará copias de seguridad, considerando el tipo de información y la frecuencia con la que se debe realizar los respaldos acorde al tipo. Se ha clasificado de la siguiente manera:

Tipo de información	Frecuencia
BDD	Diario
Código fuente	En cada cambio de versión
Proyectos	Mensual, o al realizarse cambios importantes
Informes e Investigaciones	Mensual
Actas, Memorándums, oficios.	Trimestral

Art. 70. Los respaldos se deberán almacenar en servidores o discos duros externos.

Art. 71. Las copias de seguridad se realizarán al terminar la jornada de trabajo. En el caso de realizarse automáticamente de igual forma al terminar la jornada laboral se revisará que se hayan completado con éxito.

Art. 72. Los respaldos que se realicen trimestralmente serán copias por duplicado entregados a la dirección administrativa.

ESCENCIA INDIGENA LTDA. COOPERATIVA DE AHORRO Y CRÉDITO	**Manual de Normas y Procedimientos de Seguridad de la Información**	

Dominio	8. Seguridad en la operativa	**Destinatario**
Objetivos de Control	8.4 Control del software en explotación	Equipo de trabajo del departamento de sistemas
Control	8.4.1 Instalación del software en sistemas en producción	

Art. 73. Ningún funcionario puede instalar cualquier software si no está debidamente autorizado o realizado por el responsable del departamento de sistemas.

Art. 74. El personal del departamento de sistemas será el encargado del mantenimiento del software, actualizar periódicamente el software antivirus de los equipos de los usuarios, software utilitario y actualizaciones de sistemas operativos cuando exista una necesidad para hacerlo, por ejemplo cuando la versión actual ya no de soporte a los requerimientos del negocio.

Art. 75. Si es necesario actualizar software suministrado externamente, dicha actualización deberá ser monitoreada y controlada para evitar cambios no autorizados que puedan introducir debilidades de seguridad.

Dominio	8 .Seguridad en la operativa	**Destinatario**
Objetivos de Control	8.5 Gestión de la vulnerabilidad técnica	Equipo de trabajo del departamento de sistemas
Control	8.5.1 Gestión de las vulnerabilidades técnicas	

Art. 76. Analizar archivos digitales provenientes de redes externas en busca de virus o software malicioso antes de proceder a trabajar en el archivo sospechoso.

Art. 77. Capacitar al personal el uso correcto del software antivirus al analizar archivos digitales, dispositivos de almacenamiento masivo portátil, forma de operación del código malicioso, ataques a través del correo electrónico, entre otros.

Dominio	8. Seguridad en la operativa	**Destinatario**
Objetivos de Control	8.5 Gestión de la vulnerabilidad técnica	Equipo de trabajo del departamento de sistemas
Control	8.5.1 Restricciones en la instalación de software	
Art. 78. Únicamente el personal del departamento de sistemas serán los encargados en la instalación de software importante para la empresa, así como también de determinar el tiempo máximo de almacenamiento.		

Dominio	9. Seguridad en las telecomunicaciones	**Destinatario**
Objetivos de Control	9.1 Gestión de la seguridad en las redes	Equipo de trabajo del departamento de sistemas
Control	9.1.1 Mecanismos de seguridad asociados a servicios en red	
Art. 79. Se identificará y realizarán acuerdos de servicios de red en el que consten los métodos de seguridad, niveles de servicio y requisitos de gestión de los servicios que presta la empresa. **Art. 80.** Se deberá implementar un sistema de cortafuegos para proteger a la red y sus servicios de daños externos.		

ESCENCIA INDIGENA LTDA. COOPERATIVA DE AHORRO Y CRÉDITO	**Manual de Normas y Procedimientos de Seguridad de la Información**	

Dominio	9. Seguridad en la operativa	**Destinatario**
Objetivos de Control	9.2 Intercambio de información con partes externas	Equipo de trabajo del departamento de sistemas
Control	9.2.1 Políticas y procedimientos de intercambio de información	

Art. 81. Se deberán establecer políticas, procedimientos y controles de intercambio con el fin de proteger la información mediante el uso de todo tipo de servicios de comunicación.

Art. 82. Para acceder a los servidores y aplicaciones de la empresa desde una sucursal, se realizará previa autenticación y autorización efectuada en el firewall.

Dominio	10. Adquisición, desarrollo y mantenimiento de los sistemas de información	**Destinatario**
Objetivos de Control	10.1 Requisitos de seguridad de los sistemas de información	Equipo de trabajo del departamento de sistemas
Control	10.1.1 Análisis y especificación de los requisitos de seguridad	

Art. 83. La adquisición de nuevo software deberá ser justificado estableciendo las necesidades reales de los usuarios considerando las políticas públicas, caso contrario la máxima autoridad autorizará la adquisición en base a la justificación técnica.

Art. 84. El nuevo software deberá adaptarse sin problemas a los equipos actuales de la empresa.

ESCENCIA INDIGENA LTDA. COOPERATIVA DE AHORRO Y CRÉDITO	**Manual de Normas y Procedimientos de Seguridad de la Información**	

Dominio	10. Adquisición, desarrollo y mantenimiento de los sistemas de información	**Destinatario**
Objetivos de Control	10.1 Requisitos de seguridad de los sistemas de información	Equipo de trabajo del departamento de sistemas
Control	10.1.1 Análisis y especificación de los requisitos de seguridad	

Art. 85. Entre la documentación requerida del nuevo software debe constar manuales técnicos de instalación, configuración y de usuario.

Art. 86. Se deberá archivar una copia de versiones antiguas de los sistemas reemplazados junto con su documentación técnica, la misma que servirá de soporte ante contingencias.

Dominio	10. Adquisición, desarrollo y mantenimiento de los sistemas de información	**Destinatario**
Objetivos de Control	10.2 Seguridad en los procesos de desarrollo y soporte	Equipo de trabajo del departamento de sistemas
Control	10.2.1 Restricciones a los cambios en los paquetes de software	

Art. 87. Deberán existir programas que controlen los cambios en los sistemas por parte de usuarios o terceras personas.

Art. 88. Controlar el acceso a código fuente de los programas y documentación relacionada con los sistemas de información, evitando su modificación y eliminación.

Art. 89. La actualización del software es restringida a los usuarios, sólo el administrador podrá efectuarlo siempre que sea necesario y no afecte el funcionamiento de las aplicaciones de la empresa.

ESCENCIA INDIGENA LTDA. COOPERATIVA DE AHORRO Y CRÉDITO	**Manual de Normas y Procedimientos de Seguridad de la Información**	

Dominio	10. Adquisición, desarrollo y mantenimiento de los sistemas de información	**Destinatario**
Objetivos de Control	10.3 Datos de prueba	Equipo de trabajo del departamento de sistemas
Control	10.3.1 Protección de los datos utilizados en pruebas	

Art. 90. En caso que se requiera realizar pruebas relacionadas con los sistemas de información, se debe elegir cuidadosamente la información garantizando su control y protección.

Art. 91. Los datos tomados serán utilizados únicamente para pruebas de funcionamiento y no para fines ajenos y que comprometan la funcionalidad de los sistemas.

Dominio	11. Relaciones con suministradores	**Destinatario**
Objetivos de Control	11.1 Seguridad de la información en las relaciones con suministradores	Equipo de trabajo del departamento de sistemas
Control	11.1.1 Política de seguridad de la información para suministradores	

Art. 92. Se acordará con el proveedor y se documentaran los requisitos de seguridad contra los riesgos asociados con el acceso del proveedor a los activos de la organización.

Art. 93. Se deberán firmar acuerdos o contratos de confidencialidad de la información con todos los proveedores de servicios de la empresa.

Dominio	11. Relaciones con suministradores	**Destinatario**
Objetivos de Control	11.1 Seguridad de la información en las relaciones con suministradores	Equipo de trabajo del departamento de sistemas
Control	11.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores	

Art. 94. Todos los requisitos de seguridad de la información pertinentes serán establecidos y acordados con cada proveedor que pueda acceder, procesar, almacenar, comunicar, o proporcionar los componentes de infraestructura de TI para la información de la empresa.

Dominio	11. Relaciones con suministradores	**Destinatario**
Objetivos de Control	11.2 Gestión de la prestación del servicio por suministradores	Equipo de trabajo del departamento de sistemas
Control	11.2.1 Supervisión y revisión de los servicios prestados por terceros	

Art. 95. Cada servicio con proveedor deberá tener con un supervisor encargado de revisar y auditar la prestación de servicios de proveedores.

Dominio	11. Relaciones con suministradores	**Destinatario**
Objetivos de Control	11.2 Gestión de la prestación del servicio por suministradores	Equipo de trabajo del departamento de sistemas
Control	11.2.2 Gestión de cambios en los servicios prestados por terceros	

Art. 96. Los cambios en la prestación de servicios por parte de los proveedores, incluyendo el mantenimiento y la mejora de las actuales políticas de seguridad de información, procedimientos y controles, se gestionarán, teniendo en cuenta la criticidad de la información, sistemas y procesos que intervienen y re-evaluación de los riesgos.

Dominio	12. Gestión de incidentes en la seguridad de la información	**Destinatario**
Objetivos de Control	12.1 Gestión de incidentes de seguridad de la información y mejoras	Equipo de trabajo del departamento de sistemas
Control	12.1.1 Responsabilidades y procedimientos	

Art. 97. Todos los funcionarios, contratistas y terceros tienen la responsabilidad de reportar cualquier evento en la seguridad de la información o debilidad sospechosa al tiempo de detección del incidente.

Art. 98. La coordinación de sistemas deberá elaborar un procedimiento formal para el reporte de eventos de seguridad de la información junto con un procedimiento de respuesta ante el incidente

Dominio	12. Gestión de incidentes en la seguridad de la información	**Destinatario**
Objetivos de Control	12.1 Gestión de incidentes de seguridad de la información y mejoras	Equipo de trabajo del departamento de sistemas
Control	12.1.2 Notificación de puntos débiles de la seguridad	

Art. 99. La notificación deberá ser documentada con detalle de la persona quién notifica, cargo que desempeña, posible fallo, hora del incidente, mensaje en pantalla u otro detalle relevante. Ejemplos de lo que se debe notificar.

- Perdida del servicio, del equipo o de las prestaciones de la empresa.
- Mal funcionamiento del hardware y software o sobrecarga del sistema.
- Errores humanos
- Incumplimiento de las políticas de directrices impuestas.
- Violación de las disposiciones de seguridad en cualquier aspecto.
- Cambios no controlados en el sistema.

Art. 100. Por ningún motivo los individuos que detecten las fallas o los eventos de seguridad deben tratar de explotar las debilidades o intentar solucionar los problemas.

ESCENCIA INDIGENA LTDA. COOPERATIVA DE AHORRO Y CRÉDITO	**Manual de Normas y Procedimientos de Seguridad de la Información**	

Dominio	12. Gestión de incidentes en la seguridad de la información	**Destinatario**
Objetivos de Control	12.1 Gestión de incidentes de seguridad de la información y mejoras	Equipo de trabajo del departamento de sistemas
Control	12.1.3 Valoración de eventos de seguridad de la información y toma de decisiones	
Art. 101. Realizar un diagnóstico para determinar si se trata de un incidente aislado, mal funcionamiento, negligencia o mal uso de los activos y poder dar una solución adecuada.		

Dominio	12. Gestión de incidentes en la seguridad de la información	**Destinatario**
Objetivos de Control	12.1 Gestión de incidentes de seguridad de la información y mejoras	Equipo de trabajo del departamento de sistemas
Control	12.1.4 Respuesta a los incidentes de seguridad	
Art. 102. Deberá darse soluciones rápidas, oportunas y eficientes a todos los incidentes de seguridad reportadas en las estaciones de trabajo. **Art. 103.** Capacitar al funcionario sobre el adecuado uso de los recursos y realizar el seguimiento del punto de falla.		

ESCENCIA INDIGENA LTDA. COOPERATIVA DE AHORRO Y CRÉDITO	**Manual de Normas y Procedimientos de Seguridad de la Información**	

Dominio	12. Gestión de incidentes en la seguridad de la información	**Destinatario**
Objetivos de Control	12.1 Gestión de incidentes de seguridad de la información y mejoras	Equipo de trabajo del departamento de sistemas
Control	12.1.5 Aprendizaje de los incidentes de seguridad de la información	

Art. 104. Todas las anomalías y su tratamiento deberán ser documentadas con el fin de que sean un soporte para generar respuestas eficientes en el futuro.

Art. 105. Una vez solucionado los incidentes de seguridad es importante analizar las causas que produjeron dichos acontecimientos, analizando las causas, consecuencias y la forma de prepararse y evitar similares sucesos en el futuro.

Dominio	13. Aspectos de seguridad de la información en la gestión de la continuidad del negocio	**Destinatario**
Objetivos de Control	13.1 Continuidad de la seguridad de la información	Equipo de trabajo del departamento de sistemas
Control	13.1.1 Planificación de la continuidad de la seguridad de la información	

Art. 106. El comité de seguridad informático coordinará las acciones de administración de la continuidad de las operaciones de los activos de información ante interrupciones imprevistas considerando los siguientes requisitos:

a) Identificar los activos de información críticos en los cuales se procesa la información.

b) Realizar un análisis de riesgos de los activos identificados anteriormente.

c) Evaluar y solucionar las fallas encontradas.

d) El plan debe ser socializado con todos los funcionarios de la empresa, explicando sus responsabilidades y tareas a realizar ante un incidente de seguridad.

Dominio	13. Aspectos de seguridad de la información en la gestión de la continuidad del negocio	**Destinatario**
Objetivos de Control	13.2 Redundancias	Equipo de trabajo del departamento de sistemas
Control	13.2.1 Disponibilidad de instalaciones para el procesamiento de la información.	

Art. 107. Deberá existir un área para procedimientos de recuperación, respaldo y restauración de la información en un tiempo aceptable.

Dominio	14. Cumplimiento	**Destinatario**
Objetivos de Control	14.1 Cumplimiento de los requisitos legales y contractuales	Equipo de trabajo del departamento de sistemas
Control	14.1.1 Derechos de propiedad intelectual	

Art. 108. Se deberá adquirir software únicamente a través de fuentes conocidas y de confianza para garantizar el uso de licencias originales.

Art. 109. Se deberá guardar las pruebas y evidencias sobre la propiedad de licencias, discos, manuales, etc.

Art. 110. Los derechos de propiedad intelectual debe ser un tema en las capacitaciones al personal de la empresa como también la prohibición de instalar cualquier software sin autorización del responsable de sistemas.

ESCENCIA INDIGENA LTDA. COOPERATIVA DE AHORRO Y CRÉDITO	**Manual de Normas y Procedimientos de Seguridad de la Información**	

Dominio	14. Cumplimiento	**Destinatario**
Objetivos de Control	14.1 Cumplimiento de los requisitos legales y contractuales	Equipo de trabajo del departamento de sistemas
Control	14.1.2 Protección de los registros de la organización	

Art. 111. Proteger los registros de bases de datos, contabilidad, transacciones y configuración de los activos y servicios ante modificaciones o destrucción. El cuidado y almacenamiento de los registros debe asegurar su disponibilidad e integridad cuando sea necesario.

Art. 112. Se deberá respaldar los registros mediante documentos impresos o almacenados digitalmente mediante procedimientos de backup.

Art. 113. Se deberán implementar controles para proteger los registros contra pérdida, destrucción y falsificación; si el almacenamiento es digital se debe usar contraseña de acceso.

Art. 114. El responsable del departamento de sistemas analizará si amerita o no almacenar los registros por un período largo de tiempo, caso contrario si los registros no aportan utilidad alguna a la institución el comité autorizará la destrucción de la información tanto digital como física.

Dominio	14. Cumplimiento	**Destinatario**
Objetivos de Control	14.1 Cumplimiento de los requisitos legales y contractuales	Equipo de trabajo del departamento de sistemas
Control	14.1.3 Protección de datos y privacidad de la información personal	

Art. 115. En todos los procesos de seguridad de la información debe asegurar la privacidad de la información tanto del personal como de los usuarios, estableciendo controles de acceso, verificación de identidad con la cédula de identidad o credencial respectiva y no revelar información personal de ninguna persona a individuos desconocidos.

Dominio	14. Cumplimiento	**Destinatario**
Objetivos de Control	14.2 Revisiones de la seguridad de la información	Equipo de trabajo del departamento de sistemas
Control	14.2.1 Cumplimiento de las políticas y normas de seguridad	

Art. 116. El coordinador de sistemas será el responsable de verificar constantemente el correcto cumplimiento de las normas de seguridad.

Art. 117. En caso de infracciones leves de la norma se capacitará al funcionario responsable y documentará el incidente para posteriores revisiones o actualizaciones de los procedimientos operativos.

Art. 118. En caso de infracciones graves de las normas se juzgará y sancionará por el gerente previo al informe entregado por el responsable del departamento de sistemas de acuerdo a la ley de la empresa.

Art. 119. Se considerarán como infracciones graves, una vez analizado por el Director Administrativo, personal Jurídico y Administrador de Sistemas, el incumplimiento al reglamento las siguientes:

a) Enviar mensajes para la difusión de noticias o correos electrónicos sin identificar claramente su autor, o enviar anónimos.

b) Hacer uso irracional de los recursos de la empresa tales como: espacio en disco, memoria, red informática, entre otros.

c) Congestionar los enlaces de comunicación o sistemas informáticos mediante la transferencia o ejecución de archivos o programas que nos están relacionados con sus funciones laborales.

d) Acceder a cualquier tipo de comunicaciones entre usuarios, como los chat, news group, Messenger, correo personal para fines ajenos a sus funciones laborales.

e) Descargar archivos o correo electrónico sin la debida revisión de virus informáticos.

f) Intentar apoderarse de claves de acceso de otros usuarios para acceder y/o modificar archivos.

g) Utilizar el servicio de internet para propósitos fraudulentos, comerciales, publicitarios, para propagar mensajes destructivos u obscenos, descargar música, visitar páginas pornográficas, juegos, etc.

h) Decodificar el tráfico de información o cualquier intento de obtención de información confidencial que se trasmite a través de la red.

i) Modificar la configuración de los programas de comunicaciones de los computadores o servidores de red sin autorización.

j) Ejecutar programas desconocidos en los computadores sin autorización de la coordinación de sistemas.

k) Dispersar cualquier tipo de virus informático que dañe los sistemas de procesamiento de información.

l) Transmitir cualquier tipo de información confidencial de la empresa bajo cualquier medio sin la debida autorización.

m) No cumplir con los avisos de precaución emitidos por el departamento de sistemas.

II. DESARROLLO DE PROCEDIMIENTOS DE SEGURIDAD

En esta sección se describen los procedimientos más significativos para conservar la seguridad de la información de la Cooperativa de Ahorro y Crédito Escencia Indígena, con la finalidad de organizar todas las actividades ejecutadas por los usuarios de la cooperativa que conlleven consigo un manejo responsable de los activos informáticos, ya sean físicos o lógicos, promoviendo de esta manera las buenas prácticas de seguridad de la información.

ESCENCIA INDIGENA LTDA. COOPERATIVA DE AHORRO Y CRÉDITO	**Manual de Normas y Procedimientos de Seguridad de la Información**	

Procedimiento	Soporte técnico para usuarios de Sistemas de Información		
Objetivo	Brindar soluciones eficaces y eficientes a los problemas presentados por los usuarios de sistemas de información, mediante asesoría técnica por parte del personal del departamento de sistemas.		
Frecuencia	Imprevista	**Código**	CSEG-PRO-01

1. Desarrollo de actividades

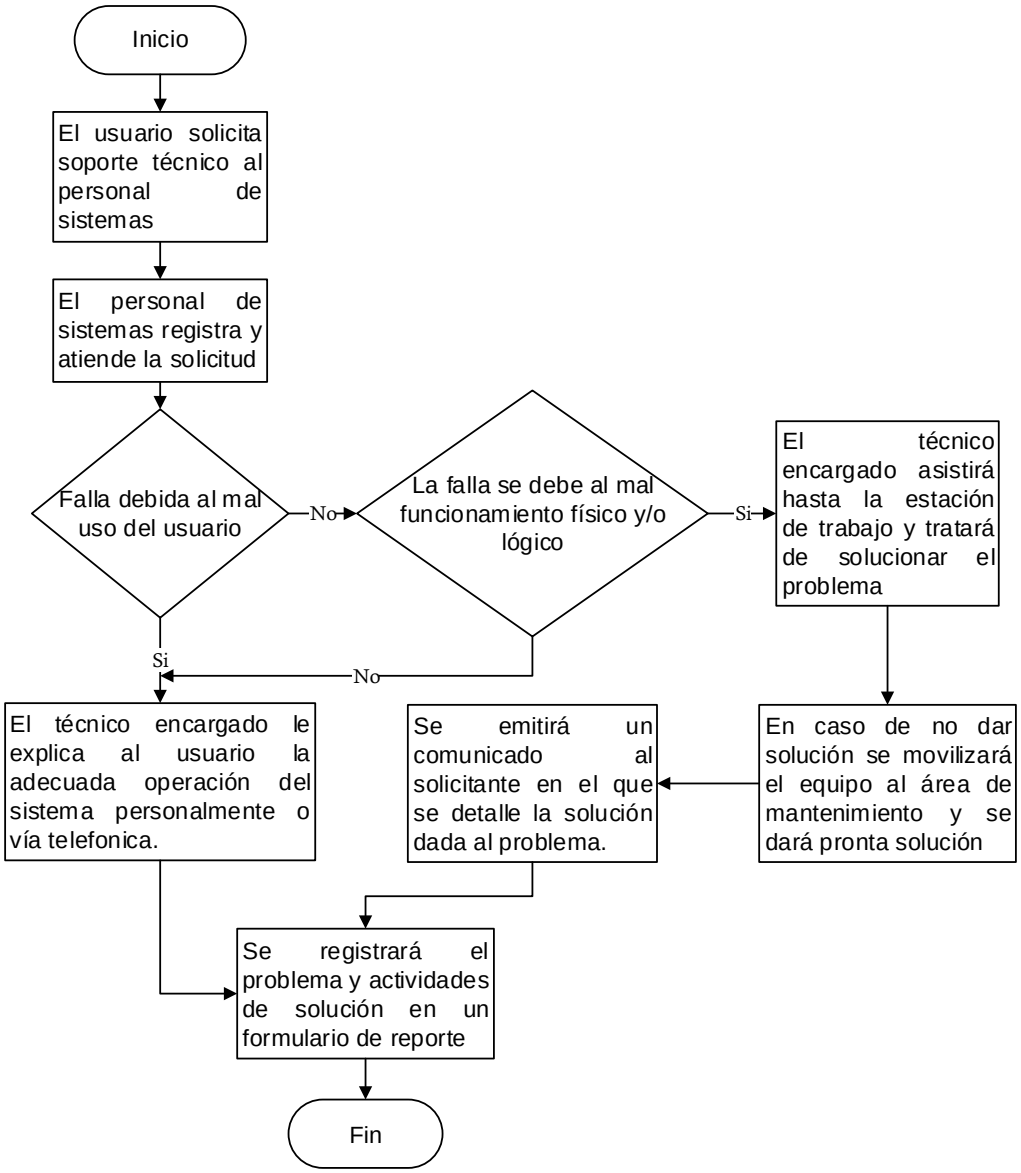
Nº Acción	Descripción
1	En caso de presentarse inconvenientes en la operación de los sistemas de información, el usuario mediante una llamada o de forma personal solicitará al personal del departamento de sistemas asesoría técnica.
2	El usuario deberá llenar una solicitud de soporte técnico en el formato **"SOLICITUD DE SOPORTE TÉCNICO EN SISTEMAS DE INFORMACIÓN"**
3	El personal técnico del departamento de sistemas registrará y atenderá la solicitud.
4	El tipo de solución dependerá de la causa del solicitante:
5	Una vez solucionado el problema se emitirá un comunicado al solicitante en el que se detallará la solución dada al problema.
6	Se Registrará el problema y las actividades realizadas en su solución.
7	Fin del procedimiento

Acción	Reacción
Falla por mal uso del operario	Explicarle al usuario la forma correcta de operación, ya sea personalmente o vía telefónica.
Falla por mal funcionamiento físico y/o lógico	Trasladarse hasta la estación de trabajo y buscar la solución al problema.
Si no se puede dar solución directa en la estación de trabajo	Se movilizará el equipo hasta el área de mantenimiento y se dará pronta solución.

ESCENCIA INDIGENA LTDA. COOPERATIVA DE AHORRO Y CRÉDITO	**Manual de Normas y Procedimientos de Seguridad de la Información**	

2. Diagrama de flujo

SOPORTE TÉCNICO PARA USUARIOS DE SISTEMAS DE INFORMACIÓN



3. Anexo Formato "SOLICITUD DE SOPORTE TÉCNICO EN SISTEMAS DE INFORMACIÓN"

Con el formato que se presenta, todos los usuarios podrán solicitar formalmente a la Coordinación de sistemas soporte técnico para los inconvenientes que se les presente, especificando sus requerimientos, con el fin de que se atienda su solicitud eficaz y eficientemente.

SOLICITUD DE SOPORTE TÉCNICO EN SISTEMAS DE INFORMACIÓN								Nº 0000
Fecha de solicitud	Día	Mes	Año	Solicitante		Dependencia:		
				Adquisición		Tutoría		
				Actualización		Cambio		
				Mantenimiento		Reparación		
	Equipo			Características		Marca		
	Accesorio					Nº de serie		
	Software					Responsable		
	Tema tutoría					tema		
Descripción breve de su solicitud: ……								
Fecha de recepción de solicitud	Día	Mes	Año	Nombre de quien recibe la solicitud		Hora:		
Para uso exclusivo del Coordinador del departamento de sistemas								
Fecha de asignación	Día	Mes	Año	Hora		Técnico responsable		
Para uso exclusivo del técnico responsable								
Fecha de entrega	Día	Mes	Año	Hora		Firma:		
Descripción breve del trabajo realizado ……								
Para uso exclusivo del usuario solicitante. Puede entregarlo al Coordinador de sistemas								
Fecha entrega	Día	Mes	Año	Hora		Firma de Recibido:		
El trabajo fue satisfactorio								
Fueron resultas sus dudas e inconvenientes								
Recomendaciones: …… ……..								

ESCENCIA INDIGENA LTDA. COOPERATIVA DE AHORRO Y CRÉDITO	**Manual de Normas y Procedimientos de Seguridad de la Información**	

Procedimiento	Creación de cuentas de usuario		
Objetivo	Asignar, modificar o eliminar un Id de usuario y contraseña cuando el usuario lo requiera.		
Frecuencia	Casual	**Código**	CSEG-PRO-02

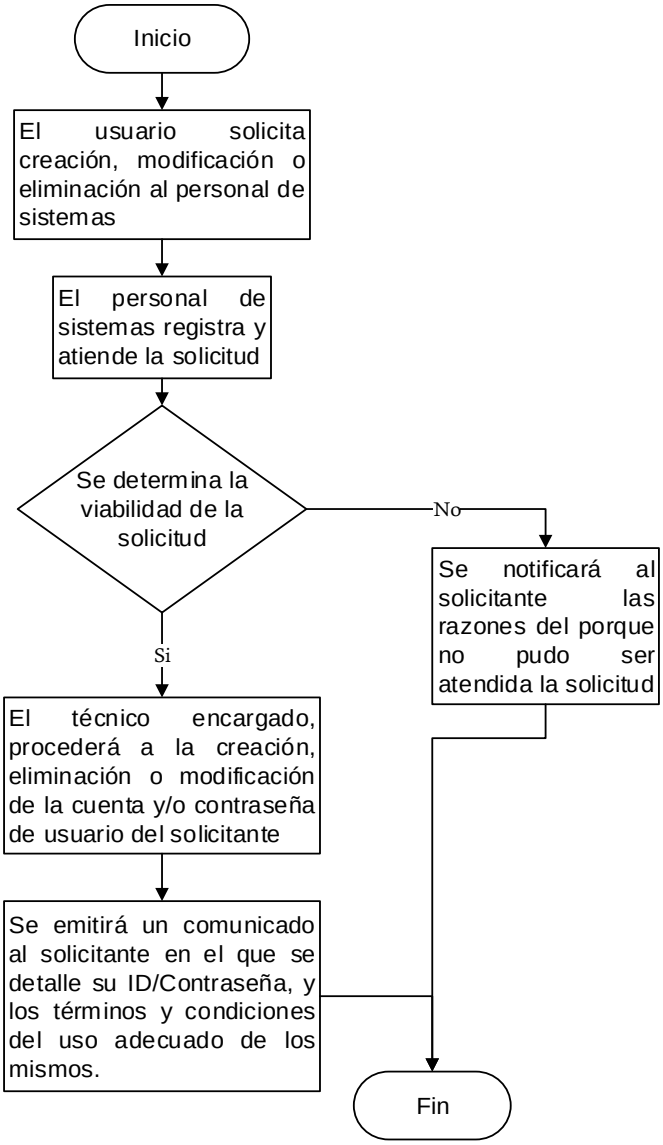
1. Desarrollo de actividades

Nº Acción	Descripción
1	Al iniciar operaciones como nuevo usuario de la cooperativa, teniendo ya una estación de trabajo, o al tener obligaciones asignadas para determinada actividad; que requiera la asignación de una cuenta de usuario, ya sea para bases de datos institucionales, correo electrónico y/o acceso a sistema operativo.
2	El usuario deberá llenar y enviar a la coordinación de sistemas la solicitud de **"CREACIÓN, MODIFICACIÓN O ELIMINACIÓN DE CUENTAS DE USUARIO"**
3	El personal técnico del departamento de sistemas registrará y atenderá la solicitud.
4	El personal encargado, determinará si es viable la creación de usuario desentendiendo del cargo que ostente el solicitante, y del acceso que según este deba tener a los sistemas de bases de datos.
5	Si es viable, se procederá a la creación de un usuario y/o contraseña para el debido acceso. Si no es viable se notificará al solicitante las razones del porque no pudo ser atendida la solicitud.
6	Una vez creado el usuario y/o contraseña se le notificará el solicitante los mismos, previo a una explicación de los términos y condiciones del uso adecuado de los mismos.
7	Fin del procedimiento

2. Diagrama de flujo

SOPORTE TÉCNICO PARA

CREACIÓN, MODIFICACIÓN O ELIMINACIÓN DE CUENTAS DE USUARIO



3. Anexo Formato "SOLICITUD CREACIÓN, MODIFICACIÓN O ELIMINACIÓN DE CUENTAS DE USUARIO"

Con el formato que se presenta, todos los usuarios podrán solicitar formalmente a la Coordinación de sistemas la creación, modificación y eliminación de cuentas de usuario, especificando sus requerimientos, con el fin de que se atienda su solicitud eficaz y eficientemente.

Solicitud de Creación de Cuentas de Usuario	Nº 0000

De: ---------- Para: ……..

Jefe o Director de departamento Jefe del departamento de Sistemas

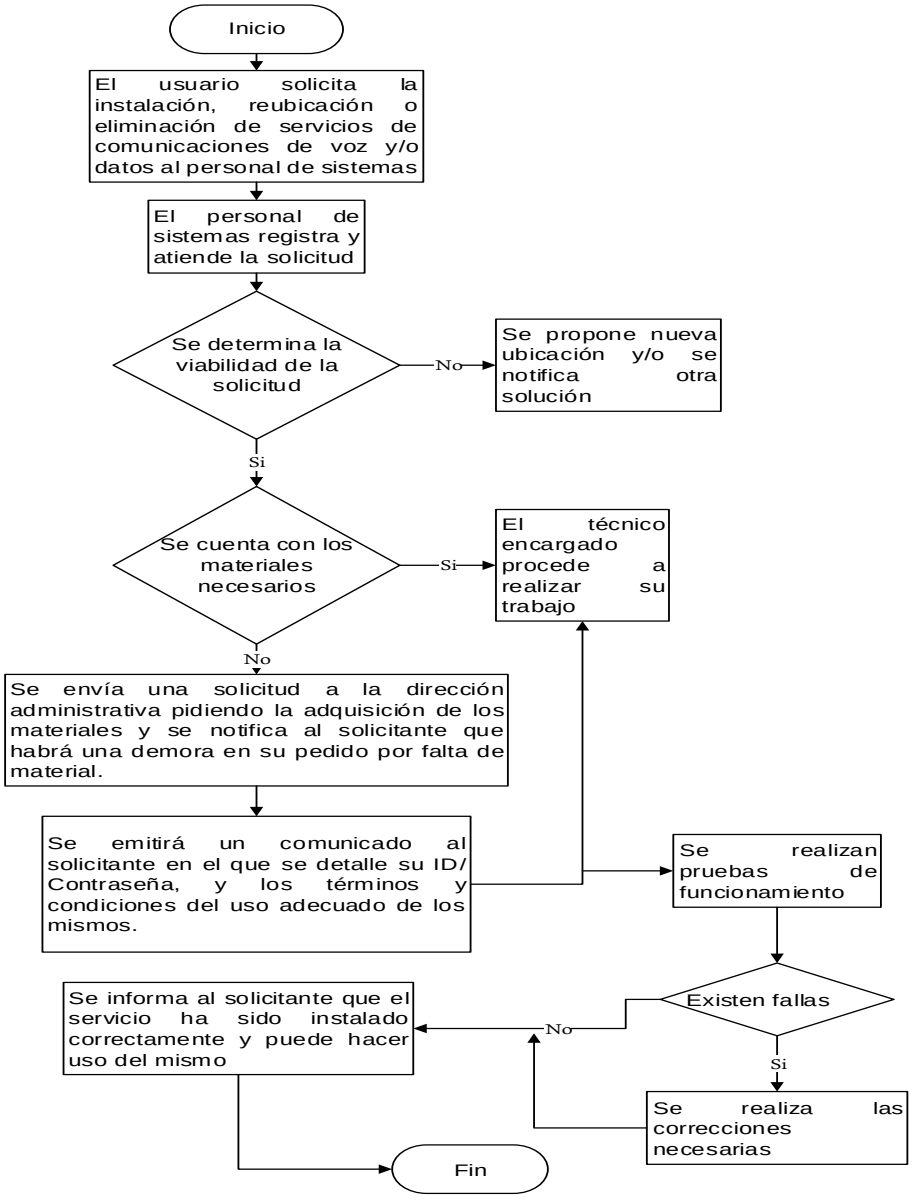
Fecha de solicitud		Día		Mes		Año		Hora			
Tipo de solicitud	Creación			Tipo de servicio	Correo electrónico						
	Modificación				Base de datos						
	Eliminación				Sistema operativo						
Datos del usuario beneficiario del ID y contraseña											
Nombres Completos					C.I.						
Cargo											
Para uso exclusivo del Coordinador del departamento de sistemas											
Fecha de asignación	Día		Mes		Año		Hora		Técnico responsable		
Para uso exclusivo del técnico responsable											
Fecha de entrega	Día		Mes		Año		Hora		Firma:		
Nombre del Solicitante											
Cargo											
Para uso exclusivo del usuario solicitante.											
Fecha entrega	Día		Mes		Año		Hora		Firma de Recibido:		
ID de Usuario							Contraseña				
Servicio											
Id Usuario							Contraseña				
Servicio											
ID de Usuario							Contraseña				
Servicio											

Procedimiento	Instalación de servicios de voz e internet		
Objetivo	Integrar a los servicios de comunicaciones de la cooperativa a los usuarios acorde a las necesidades de las áreas de la Institución.		
Frecuencia	Casual	**Código**	CSEG-PRO-03

1. Desarrollo de actividades

Nº Acción	Descripción
1	Se enviará una solicitud a la coordinación de sistemas de **"SOLICITUD DE SERVICIOS DE COMUNICACIONES".**
2	El personal técnico del departamento de sistemas registrará y atenderá la solicitud.
3	Evalúa la solicitud y la viabilidad de la misma. ¿Es viable la ubicación para la instalación?
4	Si no es viable; se propone nueva ubicación y/o se notifica otra solución.
5	Si es viable; en caso de contar con los materiales requeridos se procede a la instalación/reparación/eliminación de los servicios.
6	Si es viable; y no se cuenta con los materiales requeridos; Se envía una solicitud a la Dirección Administrativa pidiendo la adustión de los mismos; y se notifica al solicitante que habrá una demora en el servicio debido a la falta de materiales. Una vez que se tenga los materiales se procede a la instalación/reparación/eliminación de los servicios.
7	Pruebas de instalación
8	Si existen fallas, se realiza las correcciones necesarias. Caso contrario se notifica al solicitante que el servicio ha sido instalado correctamente y puede hacer uso del mismo.
9	Fin del procedimiento

2. **Diagrama de flujo SOPORTE TÉCNICO PARA SOLICITUD DE SERVICIOS DE COMUNICACIONES**



3. Anexo Formato "SOLICITUD DE SERVICIOS DE COMUNICACIONES"

Con el formato que se presenta, todos los usuarios podrán solicitar formalmente a la Coordinación de sistemas la instalación, reubicación o eliminación de servicios de voz y datos, especificando sus requerimientos, con el fin de que se atienda su solicitud eficaz y eficientemente

Solicitud de Instalación de Servicios de Comunicaciones	Nº 0000

De: ---------- Para: ……..

Jefe o Director de departamento Jefe del departamento de Sistemas

Fecha de solicitud		Día		Mes		Año		Hora			
Tipo de solicitud	Creación				Tipo de servicio	Datos					
	Re-ubicación					Voz					
	Eliminación										
Datos del usuario beneficiario del servicio											
Nombres Completos						C.I.					
Cargo											
Para uso exclusivo del Coordinador del departamento de sistemas											
Fecha de asignación	Día		Mes		Año		Hora		Técnico responsable		
Para uso exclusivo del técnico responsable											
Fecha de entrega	Día		Mes		Año		Hora		Firma:		
Nombre del Solicitante							Trabajo realizado		Instalación		
Nº Puntos de voz		Nº Punto de Datos							Reubicación		
Para uso exclusivo del usuario solicitante.											
Fecha entrega	Día	Mes	Año	Hora		Firma de Recibido:					
El trabajo fue satisfactorio											
Fueron resueltas sus dudas e inconvenientes											
Recomendaciones: …… …….. ……..											

ESCENCIA INDIGENA LTDA. COOPERATIVA DE AHORRO Y CRÉDITO	**Manual de Normas y Procedimientos de Seguridad de la Información**	

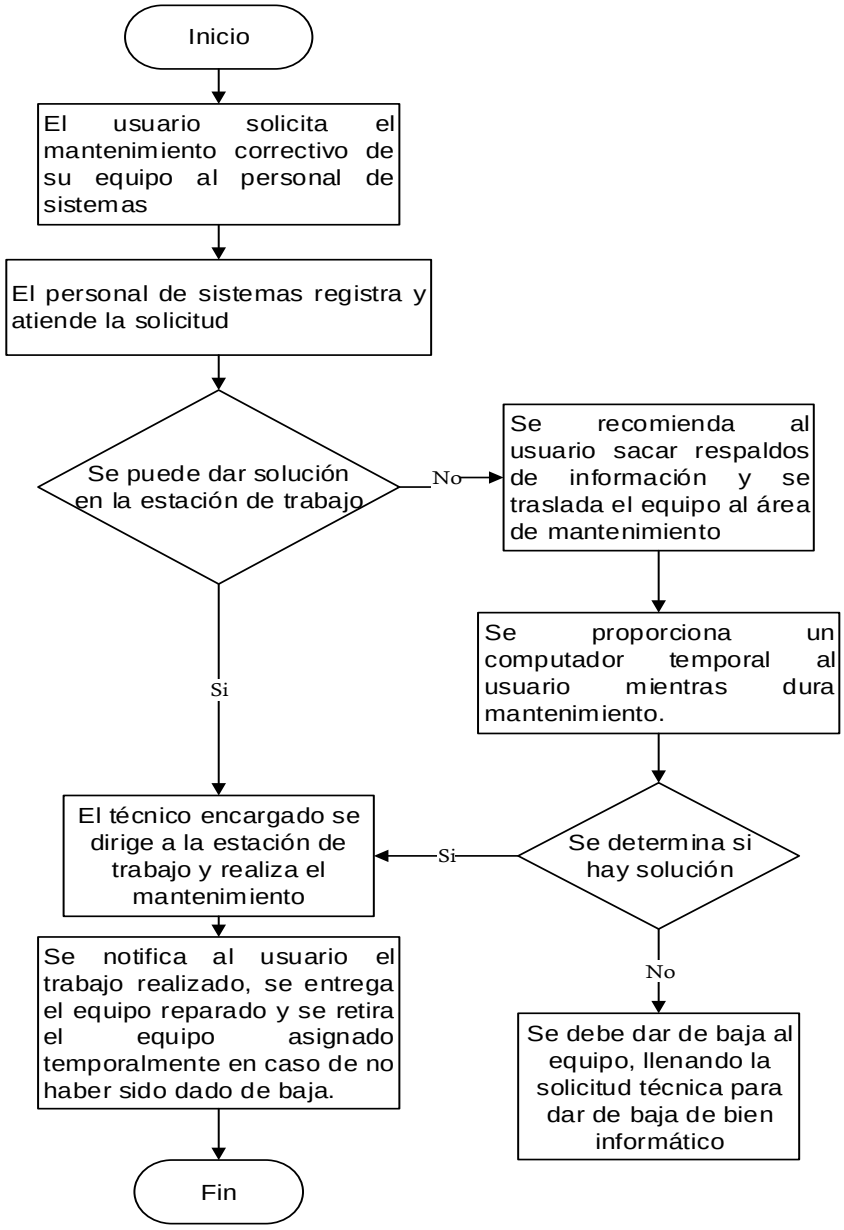
Procedimiento	Mantenimiento Correctivo		
Objetivo	Cuidar de la funcionalidad de los equipos de cómputo de todas las dependencias de la cooperativa, mediante un mantenimiento correctivo y oportuno, con la finalidad de mantener operativos dichos equipos.		
Frecuencia	Casual	**Código**	CSEG-PRO-04

1. Desarrollo de actividades

Nº Acción	Descripción
1	El usuario deberá llenar una solicitud de soporte técnico en el formato **"SOLICITUD DE SOPORTE TÉCNICO EN SISTEMAS INFORMÁTICOS"**
2	El personal técnico del departamento de sistemas registrará y atenderá la solicitud.
3	Se determinará si se puede dar solución directamente en la estación de trabajo. Caso contrario se recomienda al usuario sacar respaldos de información, y se trasladará el equipo hasta el departamento de sistemas o área de mantenimiento.
4	Mientras se da una solución se deberá proporcionar al usuario un computador momentáneo, con el fin de evitar interrupciones en el trabajo.
5	Al llevar el equipo hasta el departamento de sistemas, se determina si se puede solucionar el problema mediante mantenimiento o cambio de componentes. Si no es así se debe dar de baja al equipo, y el técnico deberá llenar el formato de **SOLICITUD TÉCNICA PARA DAR DE BAJA UN BIEN INFORMÁTICO**
6	En caso de tener solución, se realizará el mantenimiento respectivo y/o el cambio de componentes.
7	Se notifica al usuario el trabajo realizado y se le da las recomendaciones necesarias para no volver a tener inconvenientes. Se retira el equipo momentáneo que se le entrego y se vuelve a entregar el equipo, demostrándole al usuario el correcto funcionamiento del mismo.
8	Fin del procedimiento

2. Diagrama de flujo

SOLICITUD DE SOPORTE TÉCNICA EN SISTEMAS INFORMÁTICOS



3. Anexo

SOLICITUD TÉCNICA PARA DAR DE BAJA UN BIEN INFORMÁTICO				Nº 0000
Fecha	Día	Mes	Año	Dependencia:
Responsable:		Firma:		

Características del Equipo Informático						
Marca	Modelo	Nº Serie	Valor estimado	Modo de Baja	Dañado	
					Desuso	
					Irreparable	

Observaciones y/o Descripción

---------- ----------

Jefe de sistemas Técnico Responsable

Solicitante

4.2 DISEÑO DEL SISTEMA DE SEGURIDAD PERIMETRAL

Para el funcionamiento de un sistema de seguridad perimetral, es necesario la implementación de varios sistemas de control de los diferentes servicios que se prestan en la red, firewalls, proxys, anti-spam, entre otros. Por ello que la administración de todos estos sistemas se las debe centralizar y la gestión de amenazas unificadas es una excelente opción.

4.2.1 COMPARATIVA ENTRE SOLUCIÓN PROPIETARIA Y SOFTWARE LIBRE

TABLA 4. 1: Comparación de Soluciones

Característica	Gateprotect GPA 500	Software Libre
Puertos GbE	Dispone de 6 puertos	Necesita al menos 3 tarjetas de red
Prestaciones	Firewall, DMZ, IDP/IPS, Filtro de virus, filtrado web, detección de spam, IPSec/SSL, VLANs, VPN, QoS, Balanceo de carga.	Requiere configurar servidores por separado
Rendimiento de Firewall (MBit/s)	2100	Dependiente del sistema operativo
Exposición a vulnerabilidades	Muy reducidas	Propias del sistema operativo y de configuraciones incorrectas.
Costos	Por licenciamiento con soporte incluido.	Costo de aprendizaje, de instalación, de migración, de interoperabilidad.
Modo de operación	Amigable con el usuario o administrador	Complejo

Fuente: Desarrollo del proyecto

No se consideró optar por una solución por software libre debido a la carga laboral que dispone el área de sistemas.

Debido a que una solución por software libre no brinda la integración de servicios y su administración, monitoreo y mantenimiento es más complicado ya que en la mayoría de los casos se tiene que realizar vía consola y utilizar procesos más complicados y que implican más tiempo hasta poder determinar fallas y errores en el sistema; por lo cual la respuesta a errores tomaría más tiempo reflejado en la paralización momentánea de las actividades de la empresa lo cual genera pérdidas y descontento con sus socios y clientes. Y como se mencionó anteriormente se hubiera tenido que contratar una persona que se encargue del monitoreo y administración de los servidores de seguridad perimetral con lo cual representaría gastos.

Por ese motivo se consideró como mejor opción la adquisición de un equipo que pueda albergar todos los servicios necesarios para brindar la mayor seguridad a la empresa; es decir un UTM.

4.2.2 UTM (UNIFIED THREAT MANAGEMENT/GESTOR DE AMENAZAS UNIFICADAS)

Es un conjunto de características diseñadas para proporcionar la inspección de capa de aplicación, del tráfico que atraviesa una red. Al igual que en la detección y prevención de intrusiones (IDP por sus siglas en inglés), los dispositivos de seguridad que admiten características UTM descifran e inspeccionan los protocolos de capa superior para detectar tráfico malicioso o simplemente no reconocido."

Las principales características que debe tener y cumplir el Gestor de Amenazas Unificadas son:

- Cumplir con las funciones de un Firewall
- Filtrar correo, antispam
- Detección y bloqueo de malware
- Filtrar contenido WEB y URL
- Prevención y Detección de Intrusos, IDS e IPS
- Soporte de VPN y SSL[4]

[4] SSL: Secure Cockets Layer o Capa de conexión segura es un protocolo criptográfico que proporciona comunicaciones seguras.

VENTAJAS DEL UTM

La implementación de un sistema centralizado de seguridad como lo es el UTM, tiene muchas ventajas descritas a continuación:

- **Complejidad reducida**

Como UTM es una mescla de todos los productos, esto simplifica la selección de productos, la integración de los productos y el continuo apoyo hacia los mismos.

- **Facilidad de implementación**

Los productos de la UTM pueden ser fácilmente instalados y mantenidos. Todos estos productos se pueden acceder a través de sistemas remotos.

- **Flexibilidad**

UTM es flexible, con grandes y centralizados firewalls basados en software.

- **Mínima interacción del operador**

UTM reduce los casos de llamadas de auxilio del sistema y mejora la seguridad. Se utiliza un enfoque de caja negra para limitar el daño relacionado con los dispositivos de red.

- **Facilidad en la solución de problemas**

Cuando la caja negra deja de funcionar, UTM los envían fuera de su sistema para que una persona solucione los problemas. Esto lo puede hacer incluso una persona no técnica; este enfoque es mucho más útil para sistemas remotos.

Existen variedad de equipos que pueden brindar estas características pero para este proyecto se determinó que el equipo GPA 500 Gateprotect es el adecuado debido a su bajo costo en comparación a otros.

4.3.3 GATEPROTECT GPA 500

Las Amenazas de Seguridad son cada día más complejas y peligrosas, además, causan pérdidas y altos costos a las empresas. Los productos que integran soluciones efectivas contra esas amenazas son sistemas cuyo funcionamiento es difícil de entender y administrar y requiere demasiada atención y tiempo por parte de los encargados de TI, lo cual se vuelve un problema ante el incremento constante de las labores de ese departamento.

Esto inevitablemente aumenta la posibilidad y el riesgo de errores por parte de los usuarios, errores de configuración y funcionamiento en los sistemas, errores que actualmente representan más del 90% de las vulnerabilidades y brechas en la seguridad perimetral en las empresas. Sus características se muestran en el Anexo 1.

GATE PROTECT le ha dado un nuevo enfoque a este tipo de soluciones, patentando su exclusiva tecnología **eGUI** que proveé a los administradores una interfaz gráfica clara y sencilla, permitiendo una comprensión total acerca de la forma en cómo funciona el producto. El Enfoque de **GATE PROTECT** orientado al proceso permite esta facilidad de manejo, dejando atrás las complicadas sesiones de administración que requieren otros productos, mejorando de esta manera la seguridad implementada.

Con la implementación de esta solución se cumple también con lo establecido por la Superintendencia de Economía Popular y Solidaria que es la entidad que controla este tipo de empresas y se menciona en el Art. 97, en la Sección III del título III de la ley orgánica de la Economía Popular y solidaria mencionada a continuación.

Art. 97.- Exclusividad.- Únicamente las organizaciones que integran el Sector Financiero Popular y Solidario, reconocidas por la ley y debidamente autorizadas por la Superintendencia, podrán efectuar las operaciones financieras previstas en el artículo 83 de la ley. Las operaciones señaladas en el presente artículo, podrán efectuarse por medios electrónicos, ópticos, magnéticos, inalámbricos, electromagnéticos u otros similares o de cualquier otra tecnología, así como de sistemas automatizados de procesamiento de datos y redes de telecomunicaciones, que se implementarán bajo **óptimas medidas de seguridad y de conformidad con las regulaciones que se dicten para el efecto.** (Superintendencia de Economía Popular y Solidaria, 2012)**.** La certificación de regulación por parte de la superintendencia de Economía Popular y Solidaria se muestra en el Anexo 3.

4.2.4 DIAGRAMA DE RED ANTIGUO

Inicialmente la Cooperativa Escencia Indígena contaba con un equipo ClearOS y Zarafa (proxy Linux), los cuales contaban con 2 interfaces de red para Internet y LAN. Los enlaces de datos iban directamente conectados a la LAN. Estos equipos cumplían con la función de firewall pero no ofrecían toda la seguridad necesaria y su administración era compleja. Tal como se muestra en la **FIGURA 4. 1**

4.2.5 DIAGRAMA DE RED NUEVO

Con el GPA500 también se puede controlar el acceso a internet de cada usuario, teniendo la posibilidad de asignar cuotas de navegación, implementar control de aplicaciones y bloqueo de sitios web no seguros.

Los enlaces de datos se conectarán directamente al GPA500, solicitando el cambio a los proveedores respectivos. El servidor de correo ZARAFA, antes estaba conectado directamente hacia internet, con el GPA500, el equipo queda dentro de la LAN, con una configuración NAT. Se crea adicionalmente una red WiFi para invitados, con subred 192.168.X.0/24, esta red cuenta con permisos especiales para el personal administrativo en caso de conectarse a ella.

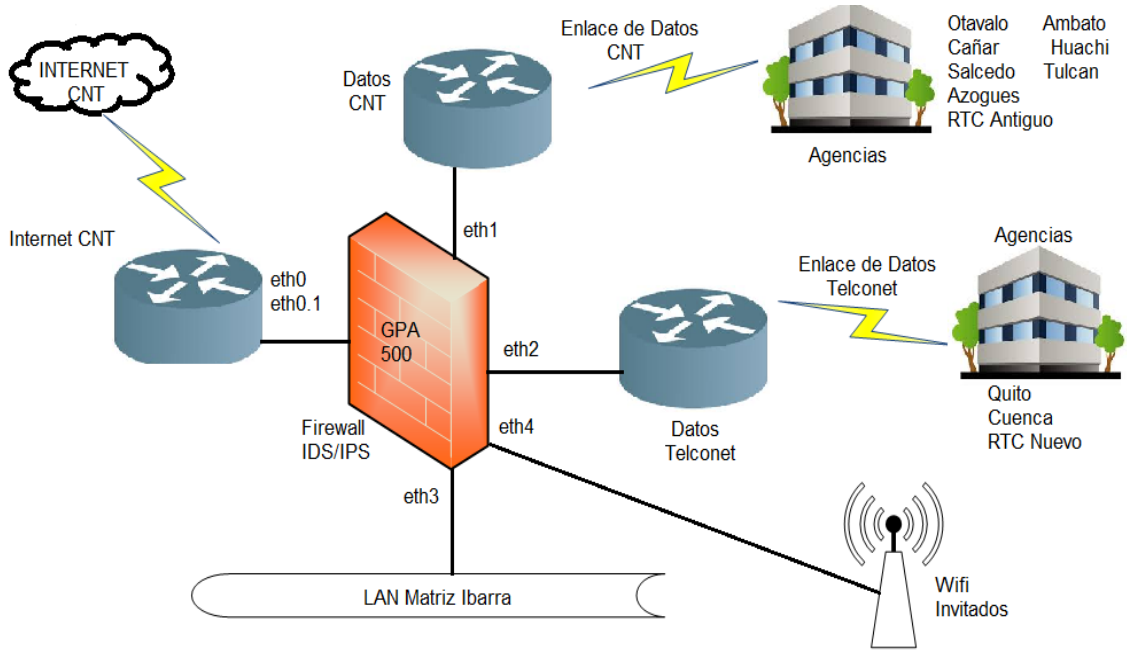


FIGURA 4. 1: Diseño de seguridad perimetral.

Fuente: Desarrollo del proyecto

CAPÍTULO V

5 IMPLEMENTACIÓN Y PRUEBAS DE FUNCIONAMIENTO

En este capítulo se describe la implementación de la DMZ, Firewall e IDS de acuerdo al diseño previo del sistema de seguridad perimetral, además se realizarán pruebas de funcionamiento para comprobar la efectividad del diseño del sistema de seguridad.

5.1 IMPLEMENTACIÓN

Como primer paso a realizar es la instalación del firmware del equipo firewall para poder acceder a todas las bondades que este equipo ofrece su instalación y la del asistente de configuración modo gráfico se muestran en el Anexo 4 y 5 respectivamente.

5.1.1 FIREWALL

Una vez instalado el firmware y el asistente de configuración modo gráfico se procede a las configuraciones del firewall.

1. Firewall-seguridad

Usando la barra de **Seguridad** en las Funciones de **Servidor** en la ventana de diálogo, se pueden cambiar las instalaciones para acceder al Servidor de Firewall esde la red externa o el Internet y expecificar cómo el Servidor de Firewall debe reaccionar a las consultas de ICMP.

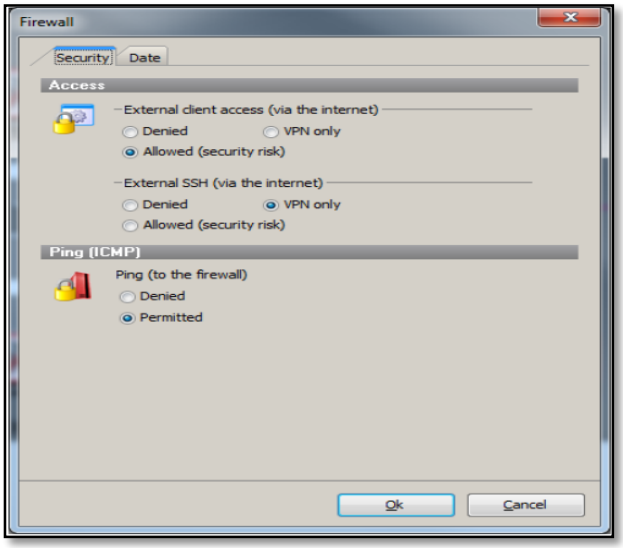


FIGURA 5. 1: Configuración del firewall

Fuente: Obtenido de administrador GPA500

En el área de Acceso está especificado que se puede acceder al servidor mediante una VPN y responde a los comandos ICMP (Ping).

2. Configuración firewall-fecha

El Servidor de Firewall gateprotect trabaja con reglas tiempo-dependientes. Por esta razón se requiere instalaciones correctas de fecha y hora. Se pueden configurar las funciones para usar un servidor de tiempo en la pestaña **Fecha**.

FIGURA 5. 2: Configuración de fecha del servidor

Fuente: Obtenido de administrador GPA500

- Seleccione una de las zonas de tiempo desde la lista Zonas de Tiempo.
- Revise el sistema de tiempo del Servidor de Firewall en los campos de Fecha y Hora.

3. Configuración de las interfaces del firewall

En esta ventana se pueden modificar distintas funciones:

- El estado de actividad de la interfaces.
- La forma en que la interface recibe la dirección IP.
- Agregar direcciones virtuales de IP.
- Establecer el color para la configuración de escritorio.

Aquí se ve que las interfaces obtienen la dirección IP de manera estática se levantan o activan únicamente las que serán utilizadas, las demás mantendrán su estado inactivo.

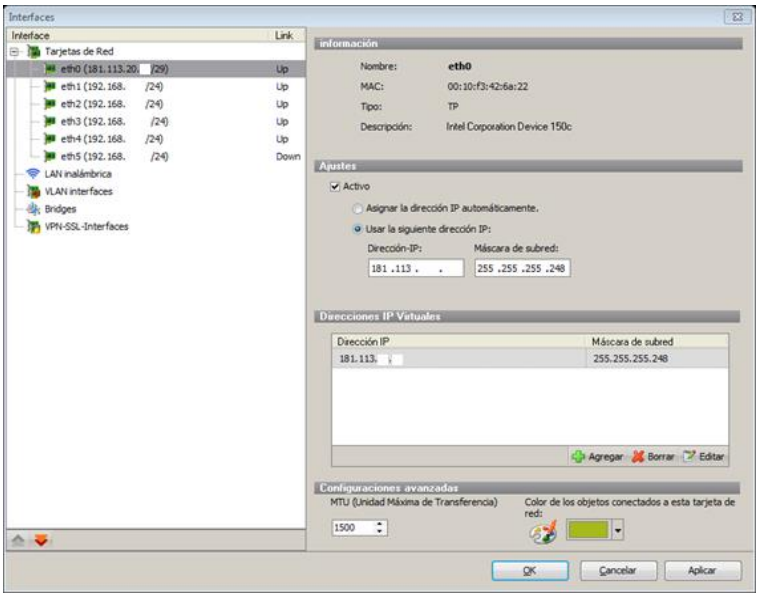


FIGURA 5. 3: Habilitar interfaces

Fuente: Obtenido de administrador GPA500

4. Uso de Ip pública principal + Ip virtual para publicación de servicios.

En esta sección se designa a la interfaz eth0 como IP pública y se configura una IP virtual para la publicación de servicios. Las IPs han sido modificadas por motivos de seguridad.

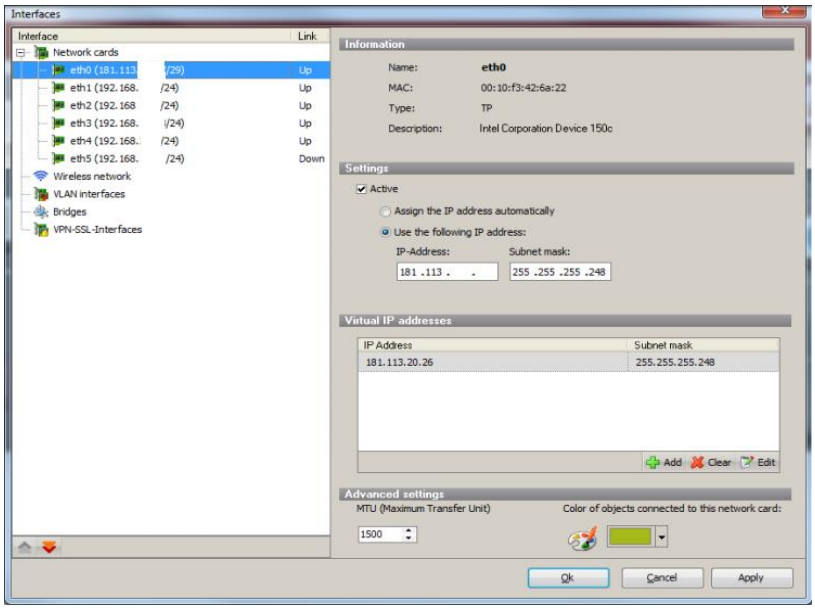


FIGURA 5. 4: Ip pública

Fuente: Obtenido de administrador GPA500

En el costado izquierdo hay un árbol que muestra tarjetas de red, VLANs, VPN-SSL-interfaces y bridges. Tras seleccionar una rama en el sitio izquierdo los detalles aparecerán en el costado derecho.

5. Definición de rutas estáticas

Aquí se asignan las subredes para cada una de las sucursales y proveedores de servicios de manera estática y asignando su puerta de enlace e interfaz que le corresponde.

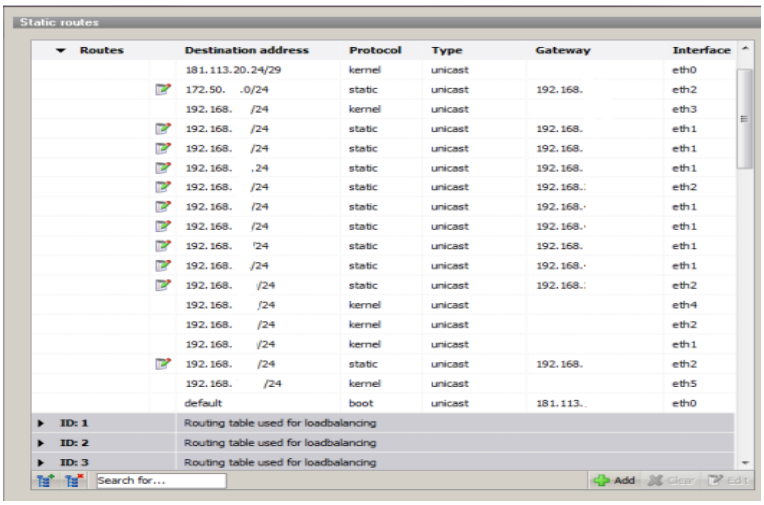


FIGURA 5. 5: Rutas estáticas

Fuente: Obtenido de administrador GPA500

6. Configuración del proveedor de internet (router connection)

Se puede acceder a la configuración del proveedor a través del Cliente de Administración Opciones > Proxy > HTTP pestaña Proxy.

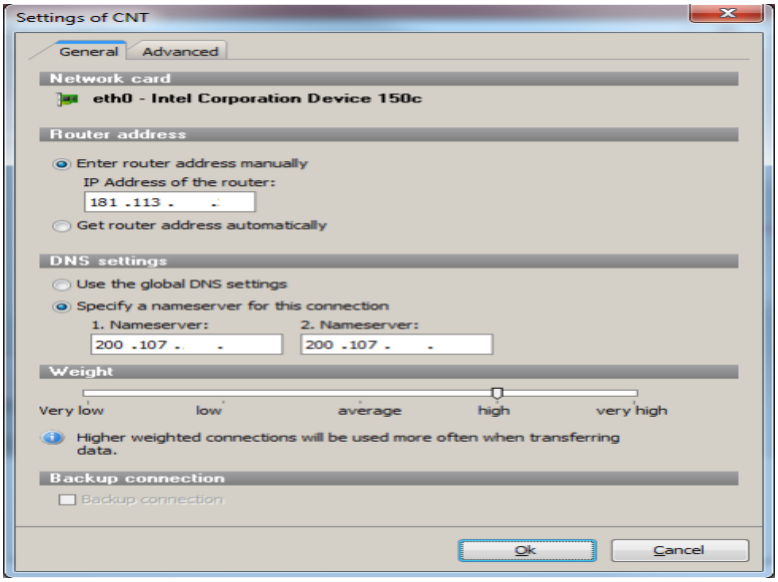


FIGURA 5. 6: Configuración internet

Fuente: Obtenido de administrador GPA500

Se configura la conexión para internet con el proveedor CNT en la cual se configura la dirección IP y sus respectivos DNS.

7. Configuración proxy modo transparente

Se puede acceder a las instalaciones de HTTP proxy a través del Cliente de Administración Opciones > Proxy > HTTP pestaña Proxy.

En esta ventana se activa el proxy en modo transparente para que el servidor firewall opere automáticamente todas las consultas hechas por el puerto 80 (HTTP) a través de proxy. También se puede configurar el caché completo de acuerdo con sus necesidades y ajustar el tamaño del caché (en MB) y los tamaños mínimos y máximos de los objetos.

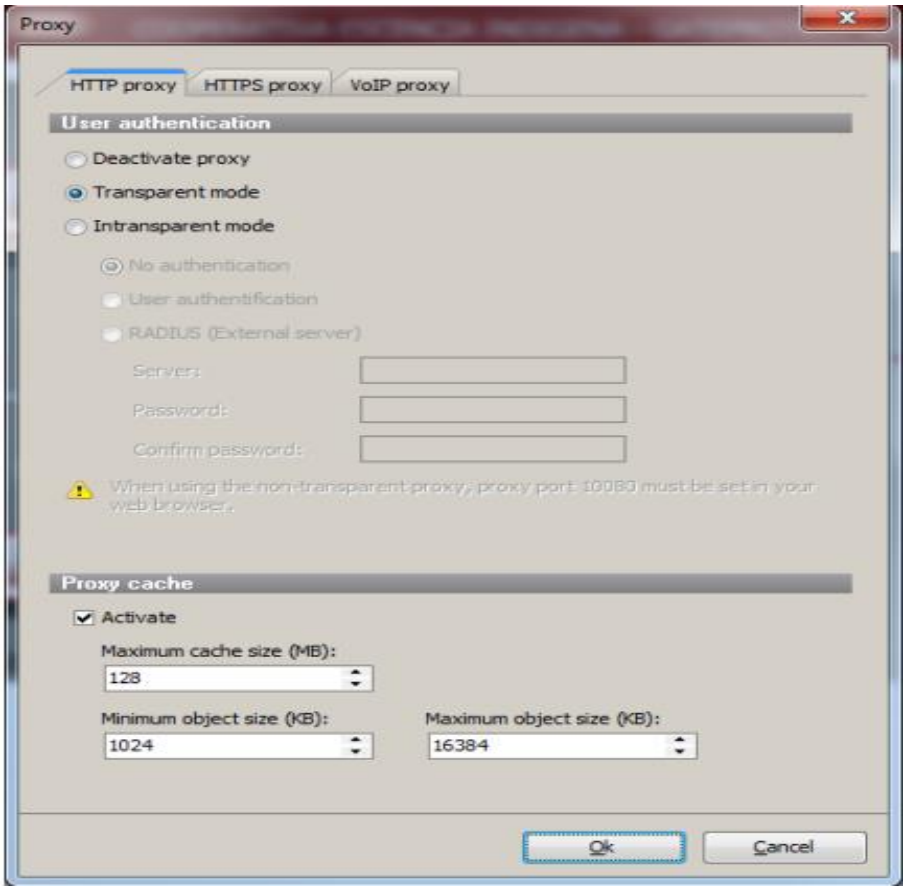


FIGURA 5. 7: Proxy transparente

Fuente: Obtenido de administrador GPA500

8. Definición de reglas de navegación (filtro URL / contenido)

En la pestaña seguridad opción Filtro URL añadir las reglas aplicadas a sitios permitidos y restringidos.

En esta ventana se presenta la lista negra; es decir los sitios que están restringidos para los operarios garantizando el buen aprovechamiento de los recursos de la red. Como ejemplo se tiene a: youtube, facebook, hotmail, entre otros.

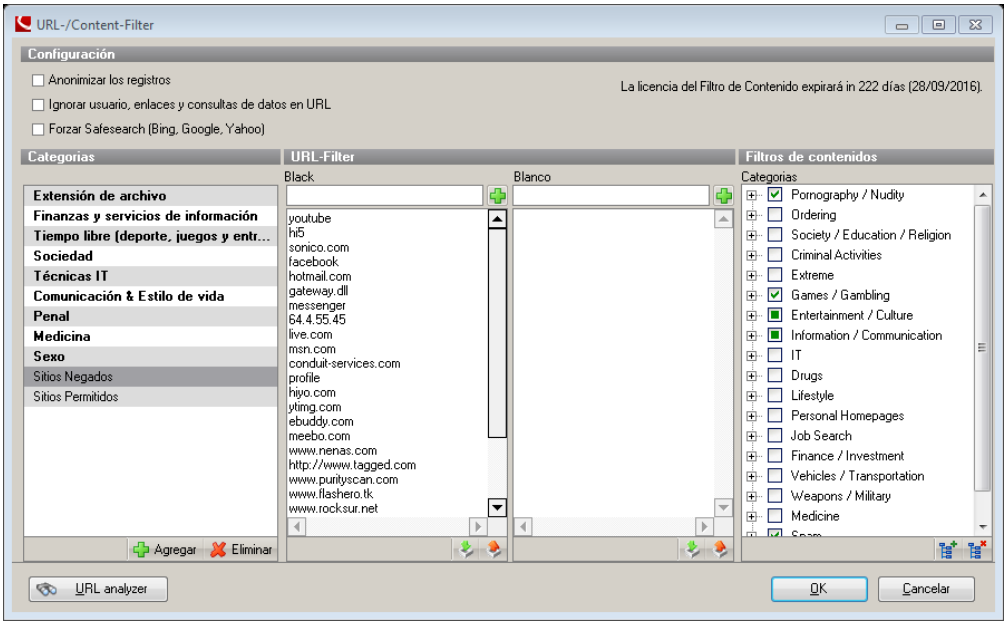


FIGURA 5. 8: Definición de reglas- Lista negra

Fuente: Obtenido de administrador GPA500

En la lista blanca en cambio se añaden todos los sitios permitidos, es decir sitios necesarios para el correcto desempeño de las labores de los operarios de la empresa. Entre los más importantes se tiene: www.conecta.com.ec, escencia.com, etc.

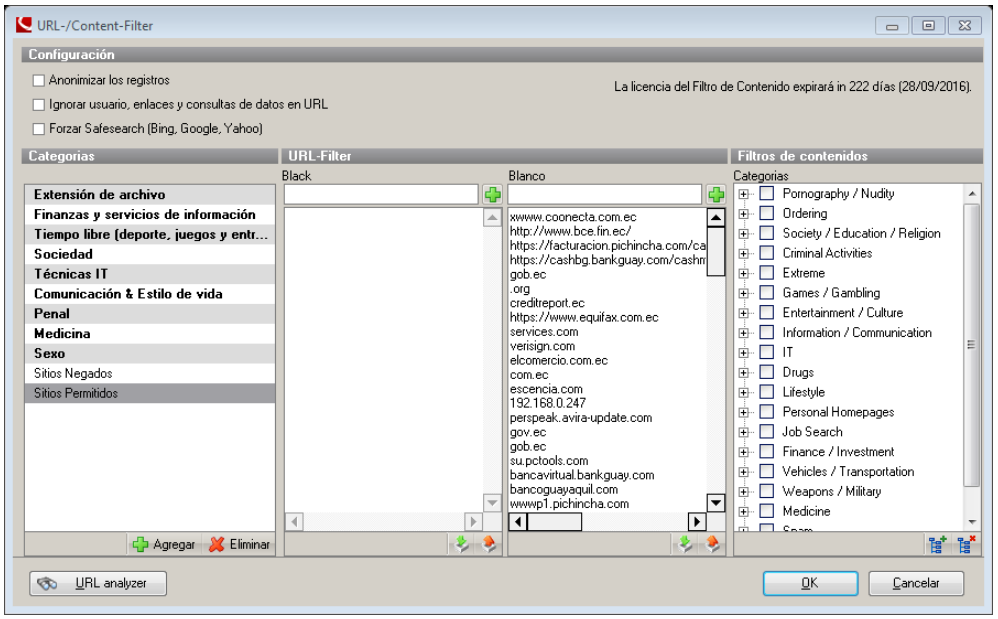


FIGURA 5. 9: Definición de reglas- Lista blanca

Fuente: Obtenido de administrador GPA500

9. Insertar objetos en el escritorio y armar la topología

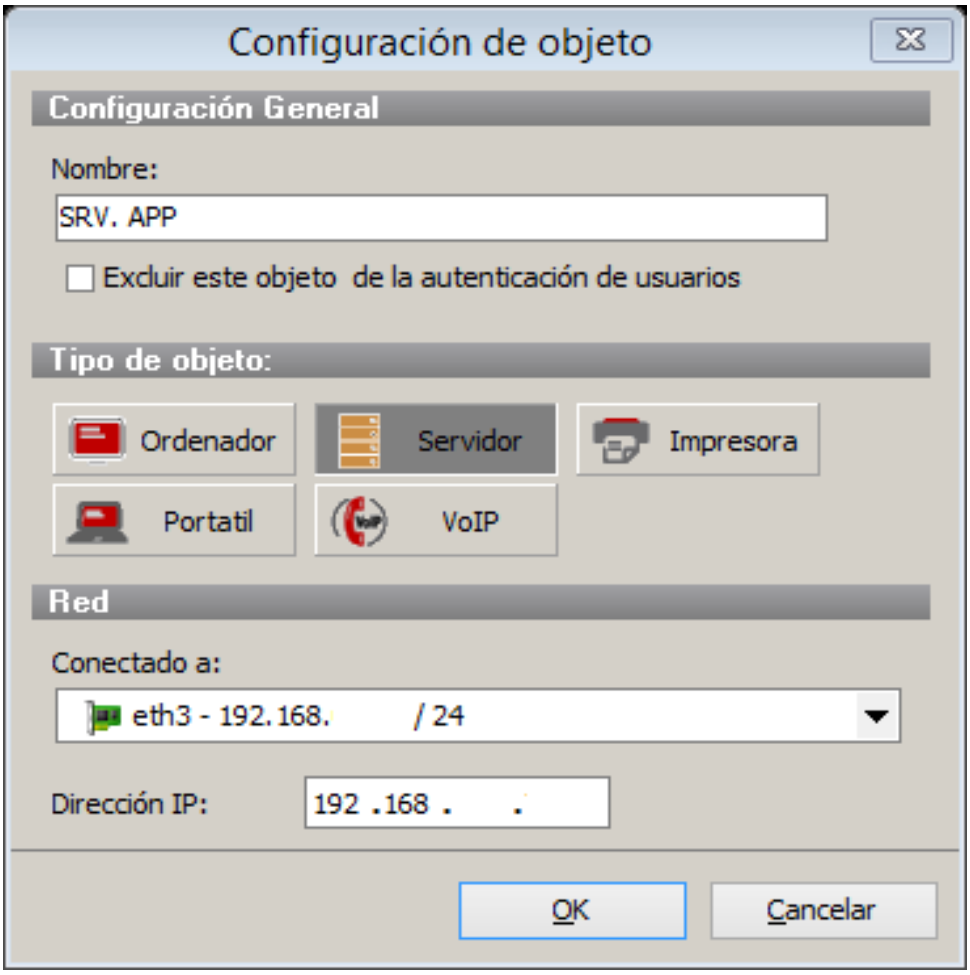


FIGURA 5. 10: Insertar objetos

Fuente: Obtenido de administrador GPA500

En la ventana anterior se ingresa el nombre del objeto y a continuación se selecciona el tipo para este caso la opción servidor, en el casillero conectado a seleccionar la interfaz a la que será conectado, finalmente asignar una dirección IP y presionar el botón OK para guardar la configuración.

El siguiente paso después de haber ingresado al menos dos objetos es enlazarlos mediante la herramienta de conexión. Posterior a ello se realiza doble click para definir las reglas.

10. Vista general de la configuración del firewall

Una vez ingresado todos los objetos que conforman la red de la empresa se tiene una topología como se muestra a continuación. Esta está dividida en dos áreas:

La primera (izquierda) permite el acceso a redes de agencias y proveedores de servicios como: servidor de base de datos conectado mediante una VPN al servidor Fitbank, también está la VPN entre la red LAN (Ibarra) y el servidor Coonecta y la conexión wifi conectado con la otra área.

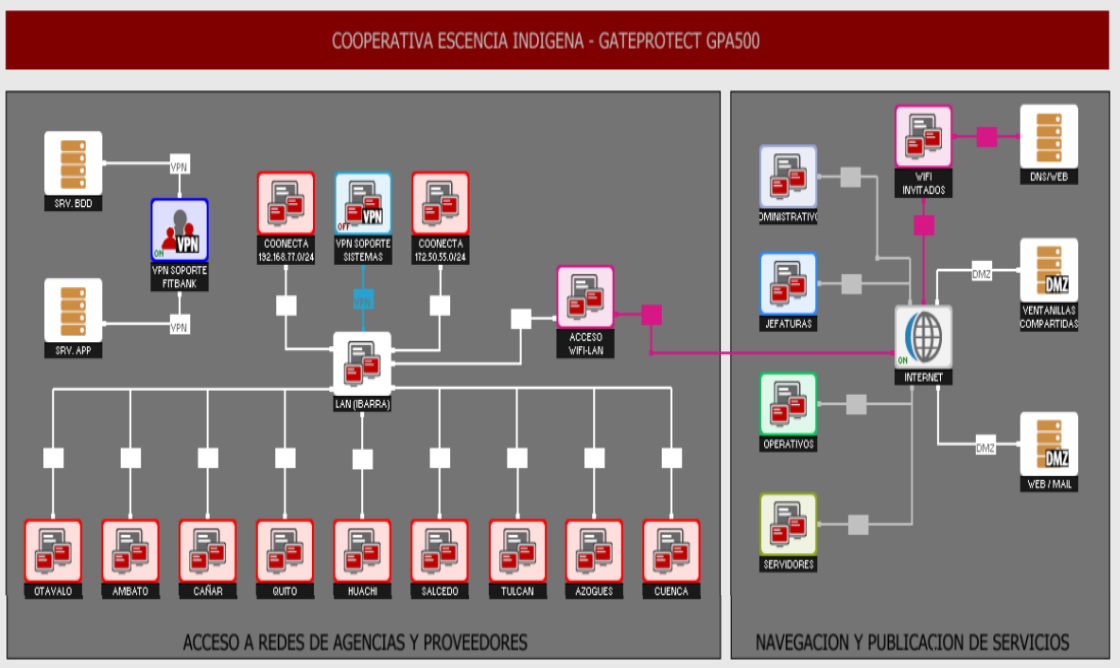


FIGURA 5. 11: Topología

Fuente: Obtenido de administrador GPA500

La segunda área permite la navegación y publicación de servicios. Esta área contiene los siguientes objetos: servidores (propios de la empresa), jefaturas, operarios, DMZ, Wifi invitados.

5.1.2 DMZ

Para la DMZ se han considerado los servidores web, correo electrónico y servidor de ventanillas. Los cuales se configuran a continuación.

1. Configuración de servidor WEB/MAIL

En esta ventana se ingresa el nombre del objeto y a continuación se selecciona opción servidor, en el casillero conectado a seleccionar la interfaz a la que será conectado, finalmente asignar una dirección ip y presionar el botón OK para guardar la configuración.

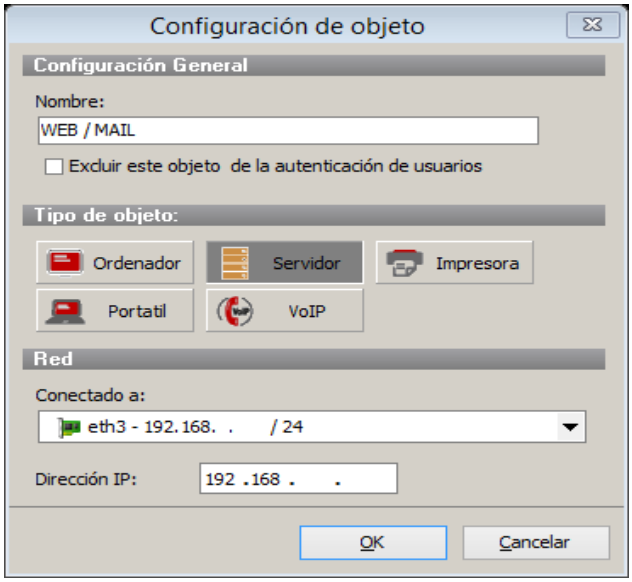


FIGURA 5. 12: Configuración servidor

Fuente: Obtenido de administrador GPA500

2. Configuración de reglas

Ingresar al editor de reglas presionando doble clic en el enlace que conecta el objeto y aparecerá la siguiente ventana en la cual se puede añadir los diferentes tipos de servicios y permisos que se le asigne lo cual se logra presionando el símbolo de una cruz de color verde ubicada en la parte inferior izquierda de la ventana.

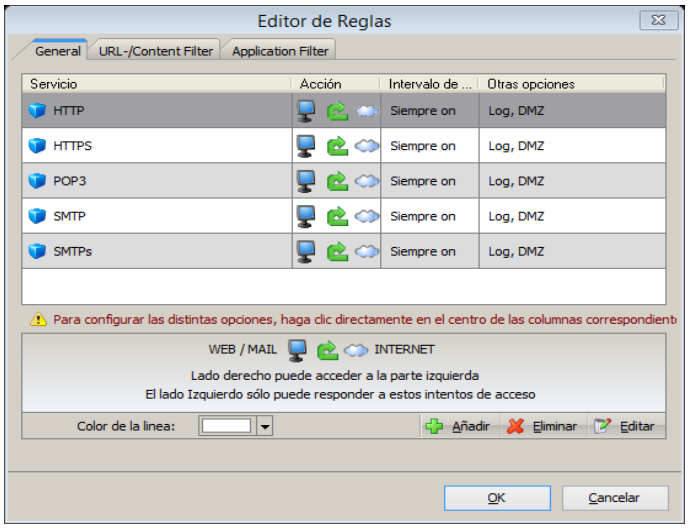


FIGURA 5. 13: Reglas del servidor Web/Mail

Fuente: Obtenido de administrador GPA500

3. Configuración servidor ventanillas

Realizar el mismo procedimiento para el servidor Web/Mail con la única diferencia de cambio de nombre y dirección IP.

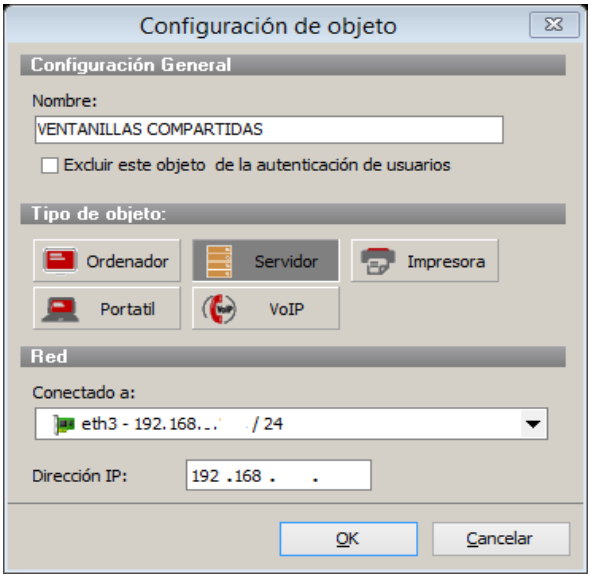


FIGURA 5. 14: Configuración servidor ventanillas

Fuente: Obtenido de administrador GPA500

4. Reglas servidor ventanillas

En el editor de reglas de igual forma se procede como en el editor de reglas para el servidor Web/Mail. En este caso el único servicio que está permitido es tcp por el puerto 8046.

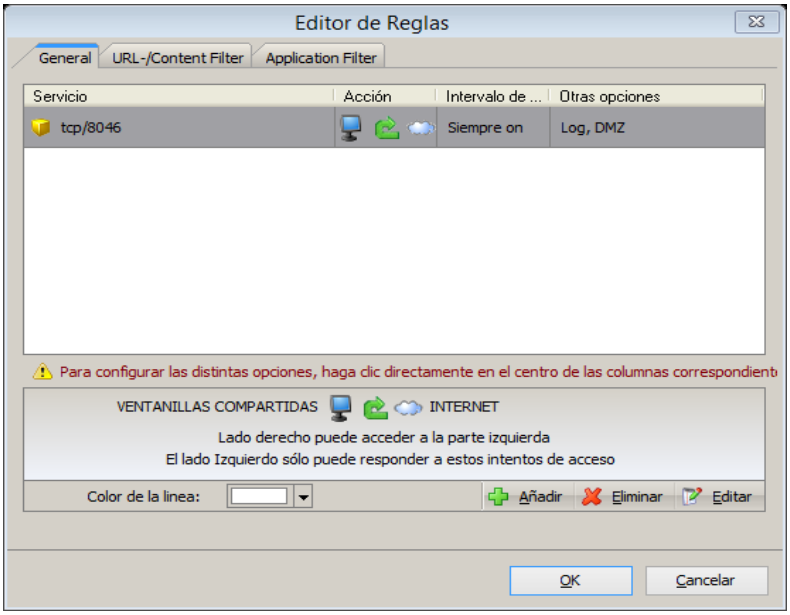


FIGURA 5. 15: Reglas servidor ventanillas

Fuente: Obtenido de administrador GPA500

5.1.3 IDS

Para acceder a la configuración del IDS/IPS se selecciona la opción **IDS/IPS** en el menú de **Seguridad.**

1. Crear perfiles de usuarios

Para configurar el IDS/IPS el Firewall gateprotect usa perfiles. Cada perfil puede ser ajustado y asignado a una interface de red. Las reglas de un perfil pueden ser ajustadas a distintos estados.

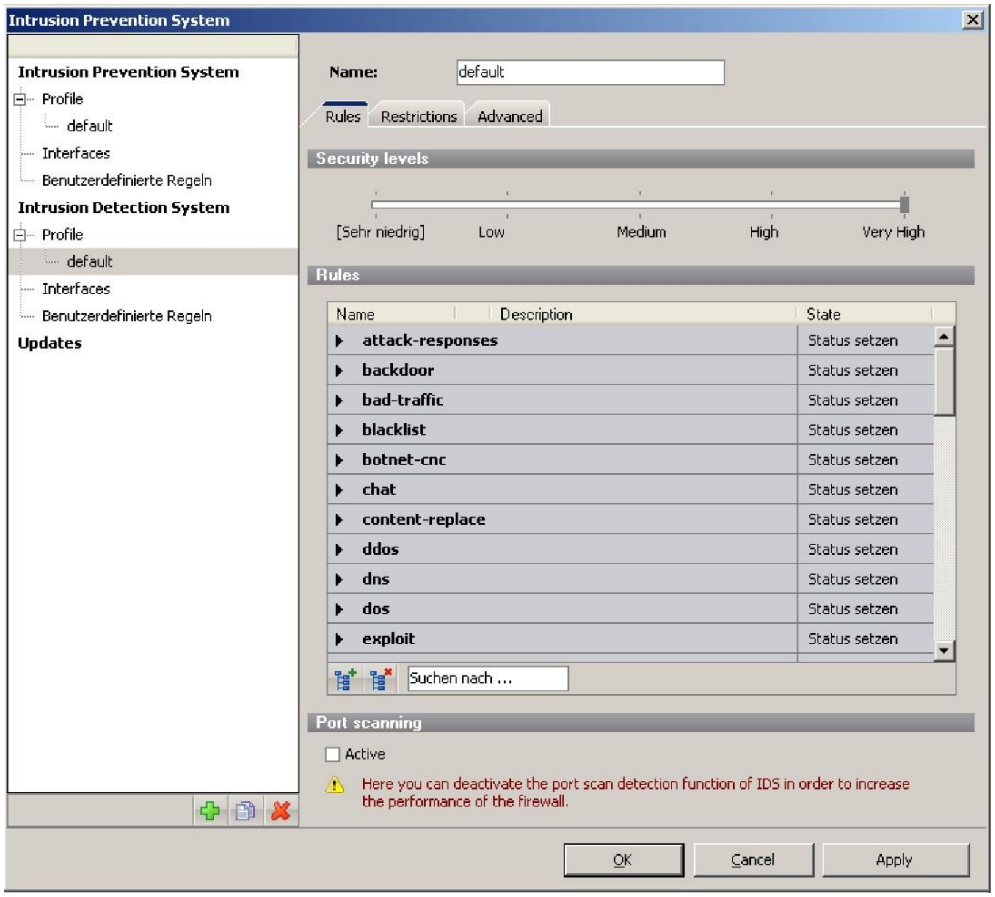


FIGURA 5. 16: Crear perfiles de usuarios

Fuente: Obtenido de administrador GPA500

El IPS ofrece 5 estados diferentes, DISABLE, LOG, DROP, DROP_LOG y REJECT para configurar reglas individualmente, el IDS tiene dos estados diferentes, LOG y DISABLE. Los estados definen cómo se define el tráfico que se apareja con las reglas.

2. Configuración de Red IDS/IPS Interna/Externa

El IDS/IPS solo produce reportes de alarma si se registran ataques en las direcciones de IP de un grupo determinado de computadores. Un grupo de computadores puede estar compuesto de computadores individuales o redes completas que están ubicadas en el área protegida de la red.

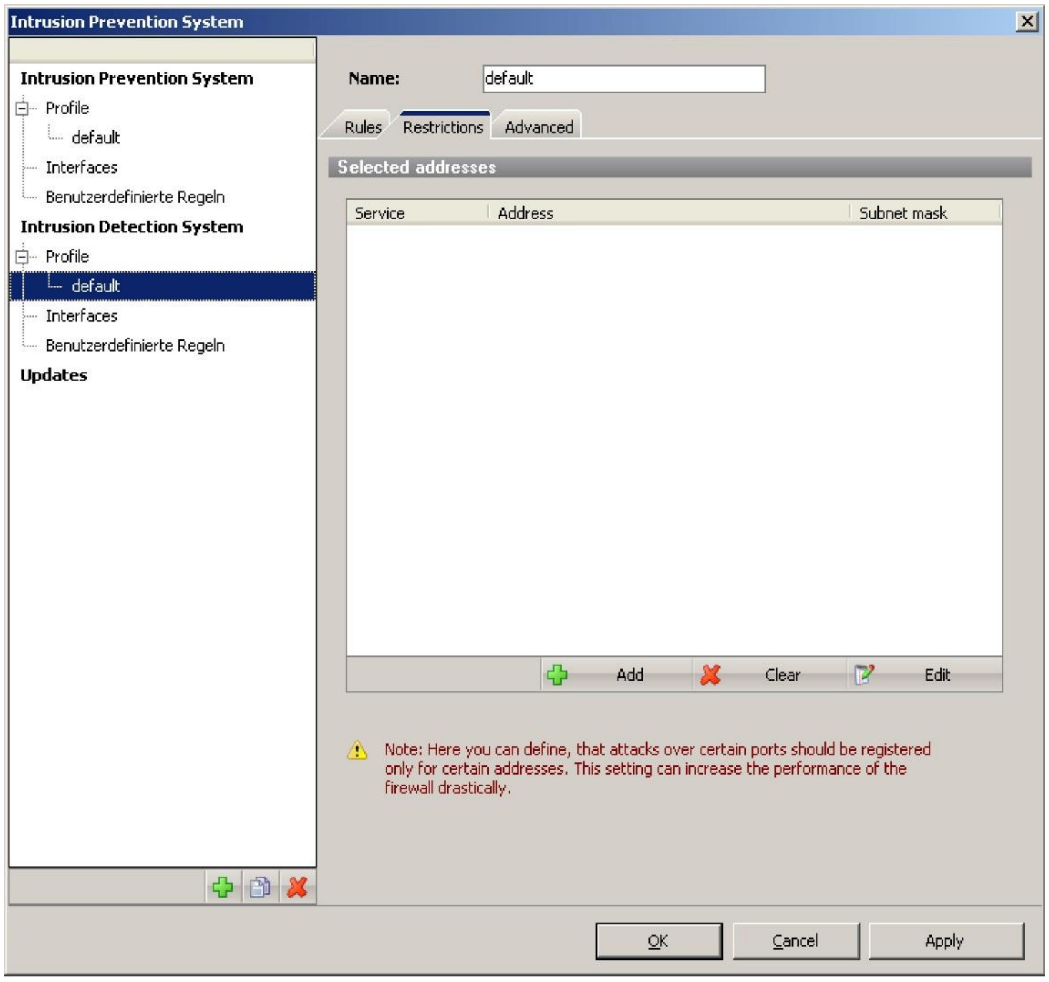


FIGURA 5. 17: Configuración de red Interna/Externa

Fuente: Obtenido de administrador GPA500

Se puede agregar o eliminar redes de computadores individuales o locales de la red interna a un grupo de computadores, o editar los grupos de computadores usando este casillero de diálogo el cual se abre al presionar el botón **Agregar**.

3. Configuración de Restricciones IDS/IPS

El Intrusion Detection System monitorea sistemas de computación especiales o redes, e.j. un servidor de red, un servidor de correo o un DMZ en particular. Se pueden ingresar los servicios y direcciones IP para este tipo de sistema computacional o red en la ventana de configuración marcada ***Restricciones***.

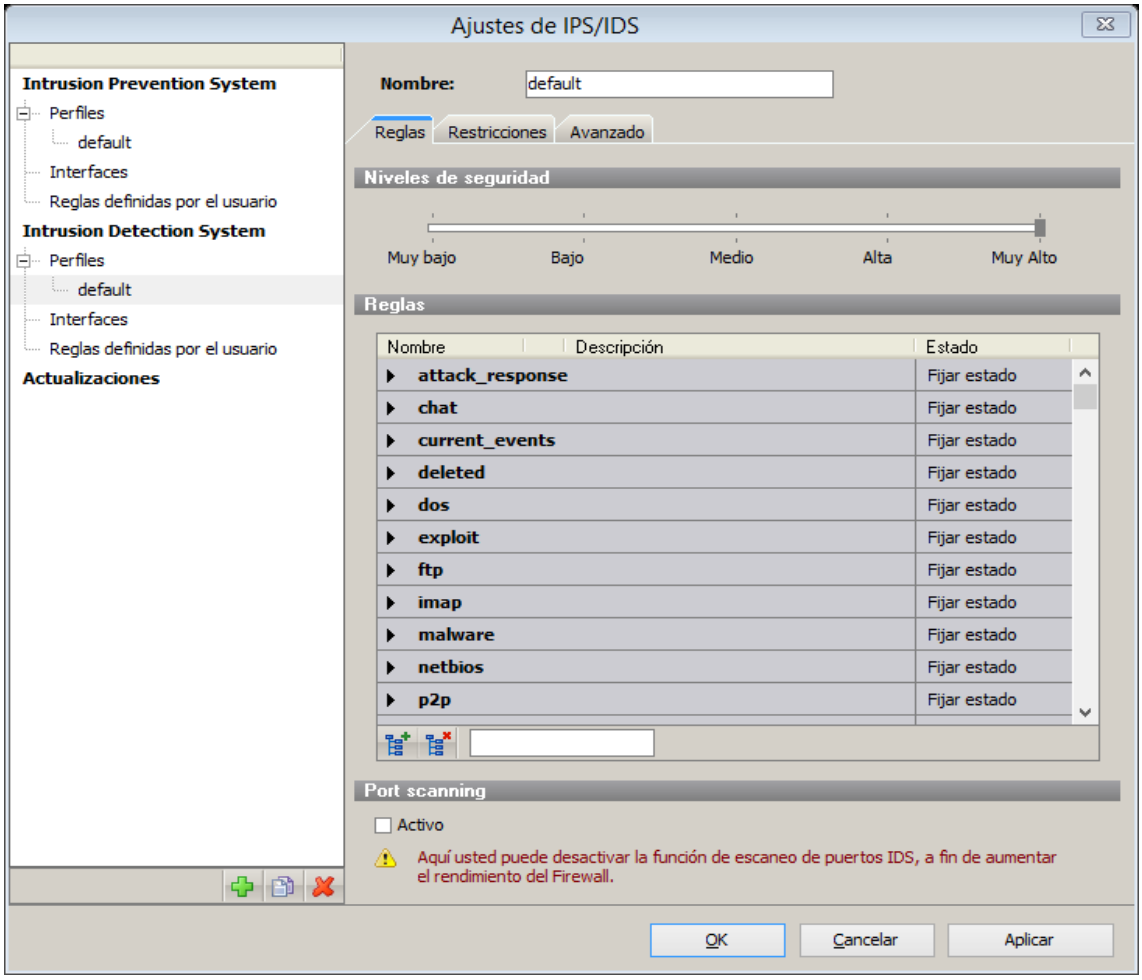


FIGURA 5. 18: Reglas IDS/IPS

Fuente: Obtenido de administrador GPA500

4. Activación del Sistema de detección y prevención de intrusos

Se accede a la ventana de diálogo de configuración de IDS/IPS seleccionando IDS/IPS desde el menú principal opción **Seguridad**.

Para activar un perfil seleccionado asígnelo a una interface.

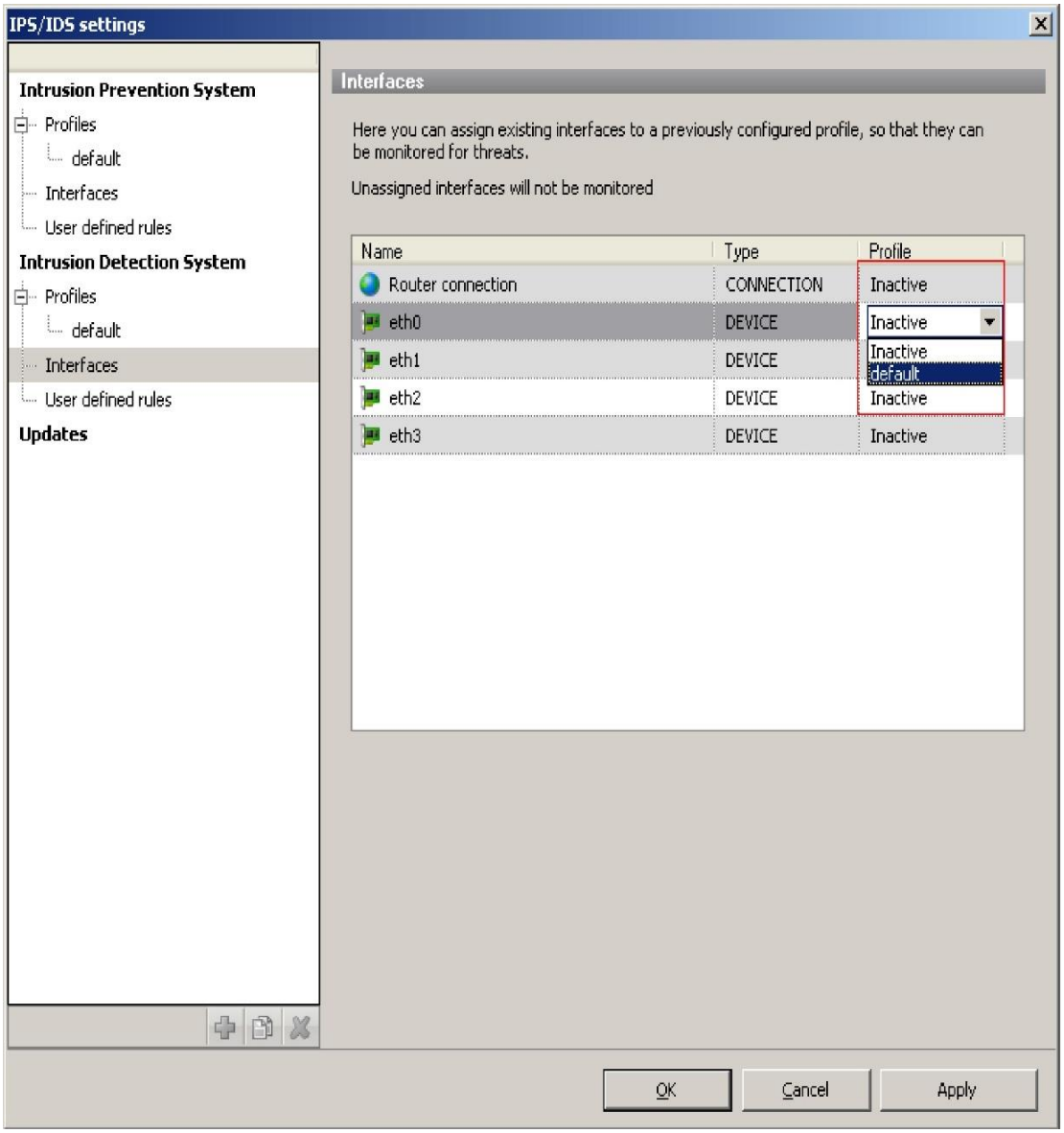


FIGURA 5. 19: Activación IDS/IPS

Fuente: Obtenido de administrador GPA500

5. Actualización de patrones IDS/IPS

Para acceder a la configuración de las actualizaciones abrir la ventana de dialogo en el menú principal **IDS/IPS** en la pestaña **Actualizaciones**.

Como los métodos de ataque están continuamente cambiando, las firmas del sistema de detección y prevención de intrusos deben ser regularmente actualizadas para reconocer semejantes ataques.

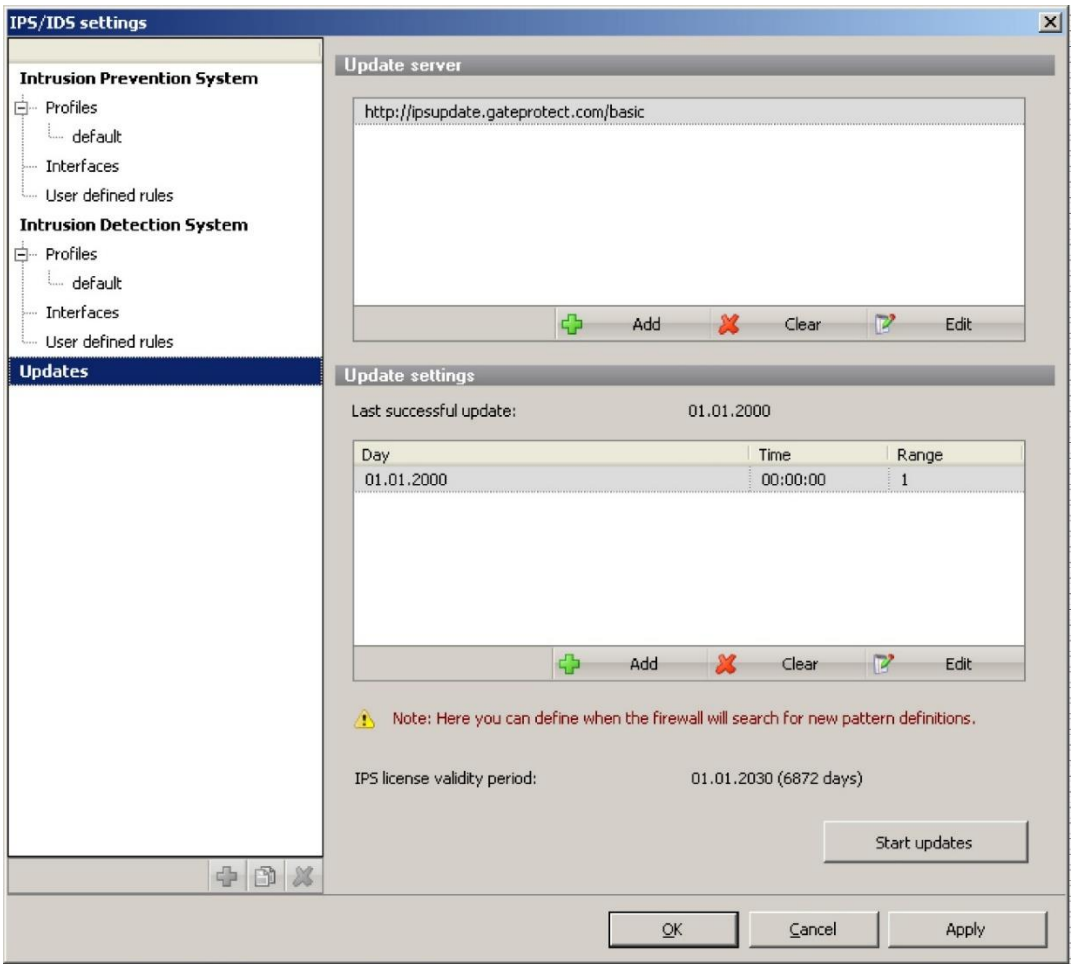


FIGURA 5. 20: Actualizaciones IDS/IPS

Fuente: Obtenido de administrador GPA500

Actualizaciones manuales

Pulse el botón **Actualizaciones manuales** para actualizar inmediatamente las firmas de IDS/IPS. El Servidor de Firewall se conecta a un servidor de firmas en Internet y carga desde ahí las firmas recientes.

Actualizaciones automáticas

Se puede especificar una lista de actualizaciones regulares en la sección **Actualizaciones Automáticas.** Abra el casillero de diálogo Instalaciones de Actualizaciones usando el botón **Agregar.** Desde ahí se pueden fijar la hora, fecha e intervalos de actualizaciones automáticas.

5.2 PRUEBAS DE FUNCIONAMIENTO

1. Estadísticas de bloqueos

En la barra de herramientas Se puede usar la barra de herramientas en las Estadísticas de Cliente para:

Imprimir las estadísticas, Cambiar el idioma de Estadísticas de Cliente para menú y uso, Obtener información sobre Estadísticas de cliente, Finalizar Estadísticas de Cliente.

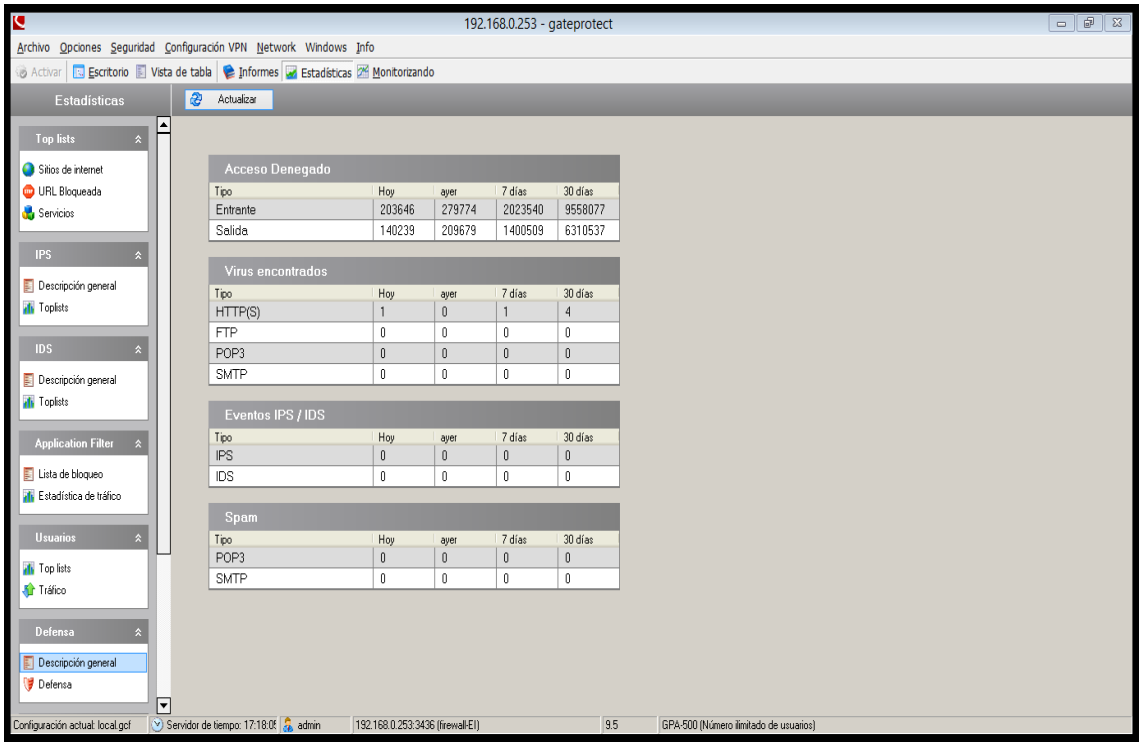


FIGURA 5. 21: Estadísticas de defensa

Fuente: Obtenido de administrador GPA500

Se pueden filtrar los resultados exhibidos dependiendo de la información de estadísticas preparada en la parte superior de la ventana de estadísticas:

Escritorio: red completa, usuarios o computadores

Período: 6, 12 o 24 horas, 7 o 14 días, 1, 3 o 12 meses

Período de auto-definición con fecha y hora para inicio y término

Ventana de tiempo: cualquier hora del día con inicio y fin

Acceso bloqueado: ingreso o salida

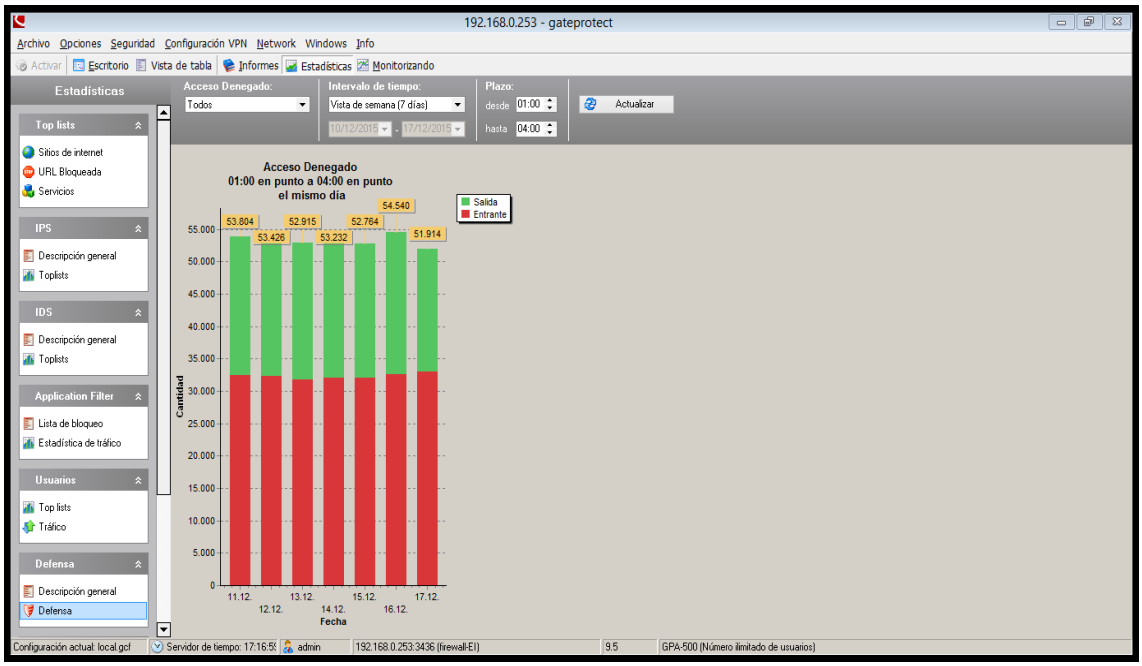


FIGURA 5. 22: Estadísticas

Fuente: Obtenido de administrador GPA500

Estadísticas por usuario, el usuario que más tráfico genera es Franz del castillo conectado a la red LAN de Ibarra.

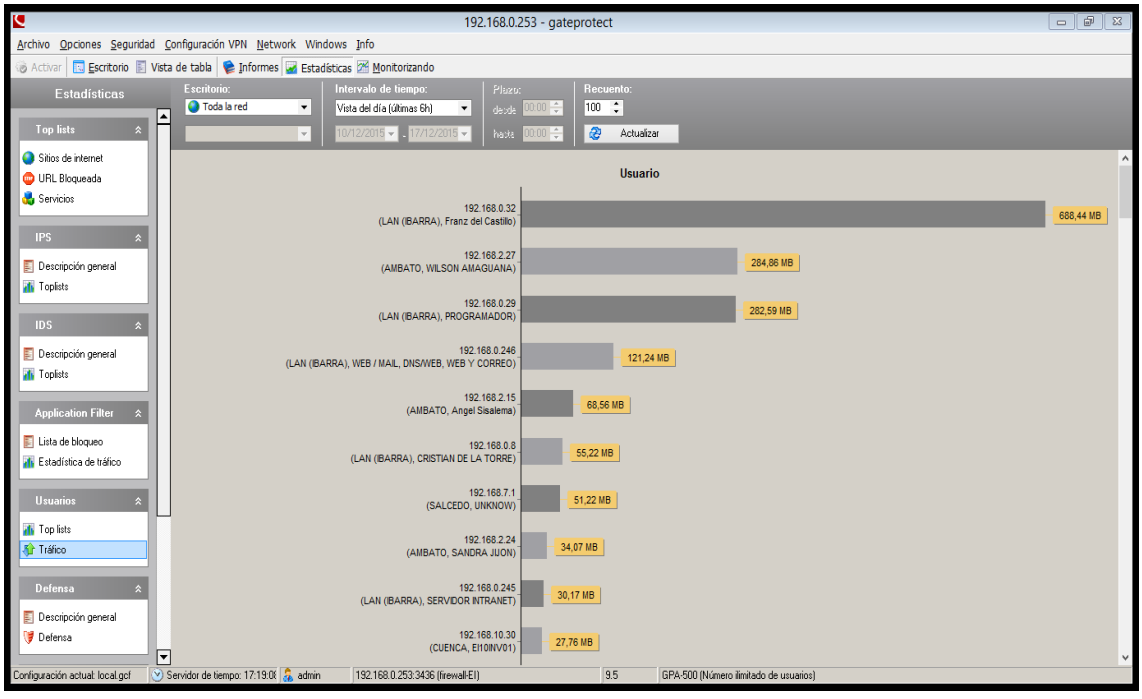


FIGURA 5. 23: Estadísticas de usuario

Fuente: Obtenido de administrador GPA500

Estadísticas por tráfico.- se observa que el mayor tráfico se genera por los servicios que utilizan los protocolos: IP/TCP/HTTP

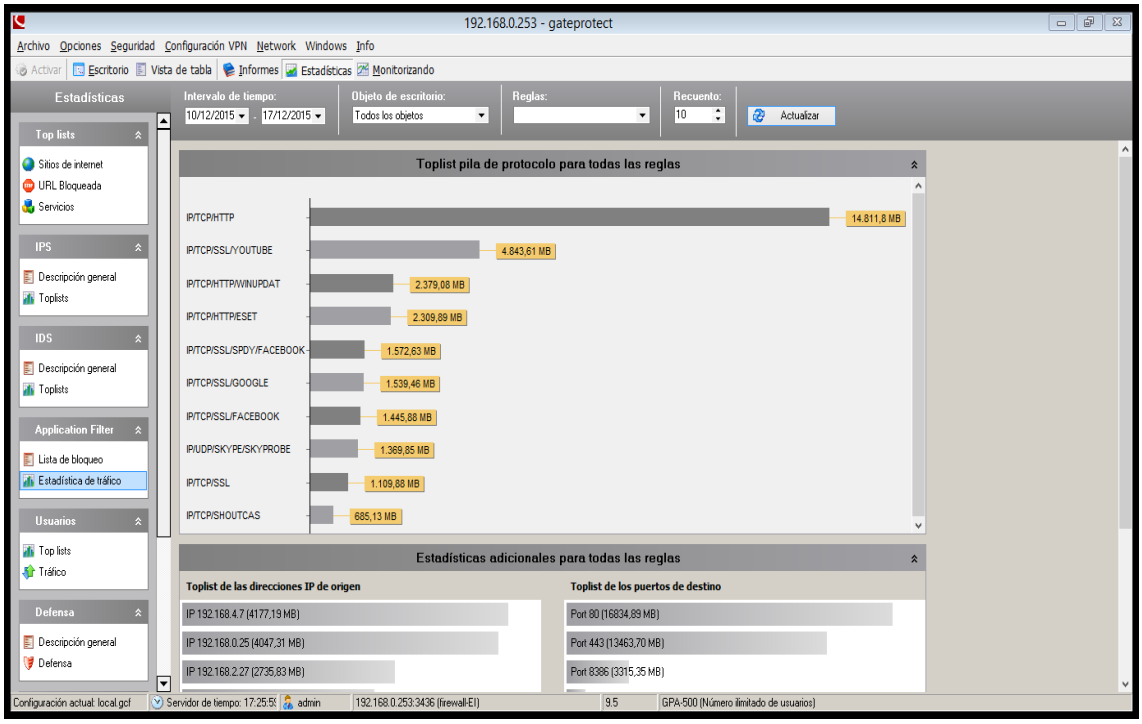


FIGURA 5. 24: Estadísticas de tráfico

Fuente: Obtenido de administrador GPA500

Intento de acceso a página bloqueada, acceso denegado correctamente.

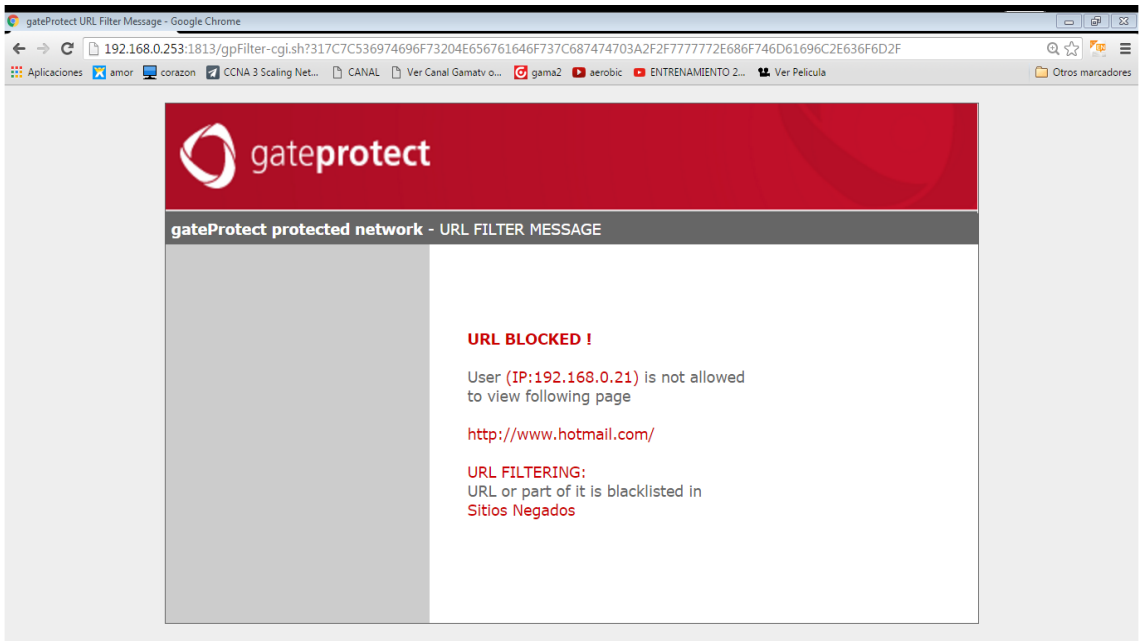


FIGURA 5. 25: Página bloqueada al usuario

Fuente: Obtenido desde el equipo de un usuario

Verificación de puertos abiertos en el servidor.- se observa que solo están abiertos los puertos necesarios y no todos como inicialmente se tenía.

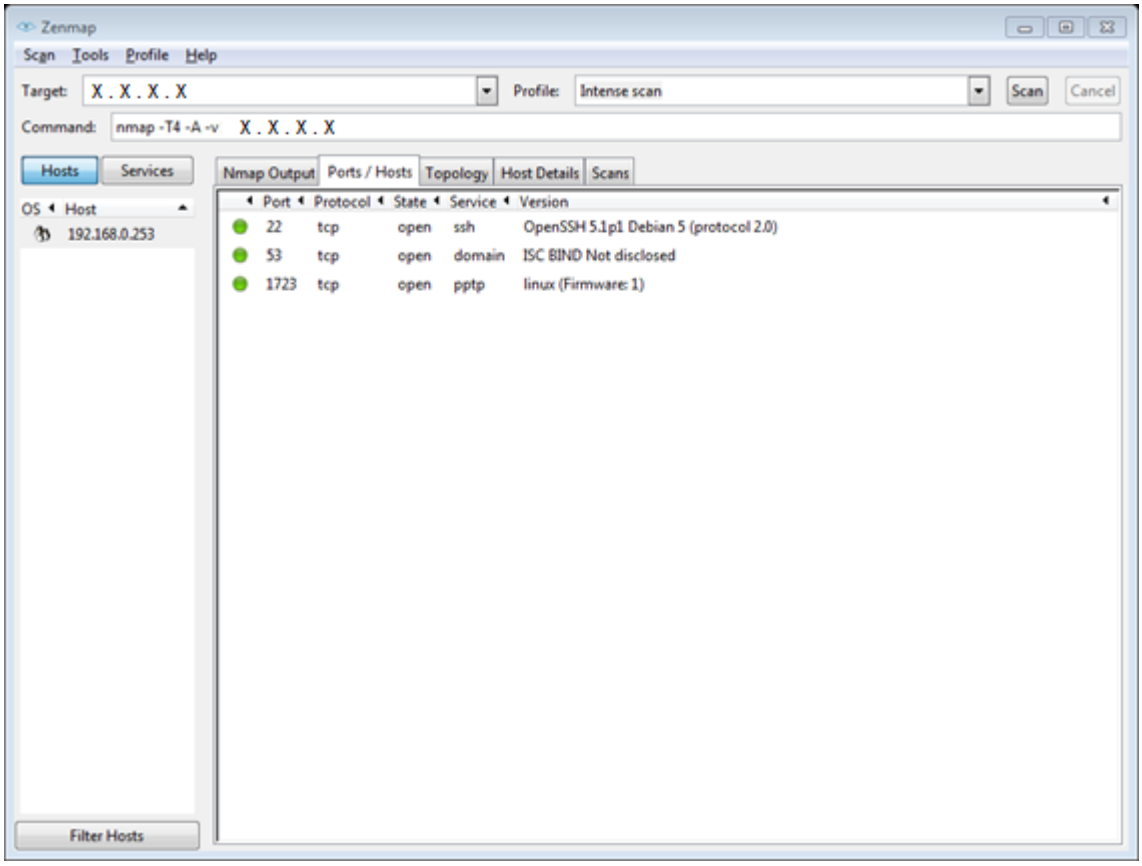


FIGURA 5. 26: Verificación de puertos del servidor

Fuente: Obtenido del software Zenmap

CAPÌTULO VI

6 ANÁLISIS DE COSTOS, CONCLUSIONES Y RECOMENDACIONES

En este capítulo se realizará el análisis de costos de los equipos que se usarán en el diseño planeado. A demás de las conclusiones y recomendaciones acordes a lo tratado.

6.1 ANÁLISIS DE COSTOS

En este último capítulo se realiza el análisis económico de los elementos utilizados en la implementación del Sistema de seguridad Perimetral en comparación de dos soluciones disponibles en el mercado.

6.1.1 COSTOS DE LA INVERSIÓN

El presupuesto del proyecto es el documento en el que consta la cantidad de dinero que se necesitará para llevar a cabo las actividades planificadas.

6.1.2 COSTO DE EQUIPAMIENTO

En este punto se detalla el valor de los equipos necesarios para la implementación de este diseño descritos en la **TABLA 6. 1**. El análisis se basó, en los equipos disponibles en el mercado nacional, las marcas más utilizadas y los precios referenciales de las mismas.

TABLA 6. 1: Costos de equipos

COSTOS EQUIPAMIENTO			
EQUIPAMIENTO	CANTIDAD	PRECIO	
		COSTO UNITARIO	SUBTOTAL
GATEPROTECT GPA 500	1	$ 4.032,00	$ 4.032,00
PC CLIENTE	1	$ 300.00	$ 300,00
TOTAL			**$ 4.332,00**

Fuente: Proforma empresa SMART HELP SOLUCIONES ver **ANEXO 2**

6.1.3 COSTOS DE INGENIERIA

En los costos de ingeniería se considera el costo del servicio de instalación y configuración del equipo mostrados en la **TABLA 6. 2**

TABLA 6. 2: Costos de Ingeniería

COSTOS INGENIERIA			
EQUIPAMIENTO	CANTIDAD	PRECIO	
		COSTO UNITARIO	SUBTOTAL
Diseño del sistema de seguridad	1	$ 400,00	$ 400,00
Instalación y configuración	1	$ 100,00	$ 100,00
TOTAL			**$ 500,00**

Fuente: Proforma empresa SMART HELP SOLUCIONES ver ANEXO 2

6.1.4 INVERSIÓN TOTAL

En la **TABLA 6. 3** se muestra el costo total para el sistema de seguridad de la empresa.

TABLA 6. 3: Inversión total.

COSTOS TOTALES DE SEGURIDAD			
DESCRIPCIÓN	UNIDAD	CANT	TOTAL
EQUIPAMIENTO	u	1	$4.332,00
INGENIERIA	u	1	$ 500,00
TOTAL			**$4.832,00**

Fuente: desarrollo del proyecto

La implementación de este proyecto tiene un valor 4032 dólares debido a que la pc para la administración ya contaba la empresa y el valor de ingeniería fue parte del desarrollo del proyecto.

El beneficio que obtiene la empresa además de los ya mencionados es que al adquirir esta solución es que al no optar por esta solución y haber optado por servidores independientes sean estos de software libre era necesario contratar una persona encargada de los servidores de seguridad perimetral ya que la carga para el departamento de sistemas es demasiada. Con esto al contratar un empleado con un sueldo mínimo de 600 dólares en los 12 meses que dura la licencia del equipo se tendría una inversión de 7200 dólares exponiéndose a fallos ya que los sistemas no resultan tan robustos como lo es la solución de gateprotect. Con la solución planteada se tiene segura la infraestructura tecnológica de la empresa y aumenta su productividad basado en tres puntos clave: reducción de tiempo, reducción de errores y reducción de costos.

6.2 CONCLUSIONES

- Se investigó la temática relacionada con el tema a desarrollar con el fin de no desviarse del objetivo planteado y presentar la mejor solución a través de diferentes fuentes bibliográficas.

- Conocer la infraestructura tecnológica de la empresa y las entrevistas con el administrador de la infraestructura tecnológica de la empresa fue el primer paso para desarrollar el proyecto ya que esto permitió conocer los riesgos y debilidades.

- La norma ISO IEC/27002:2013 no establece una metodología de análisis y gestión de riesgos informáticos, pero recomienda elegir una metodología que más se relacione con las necesidades y características de la entidad a analizar.

- El análisis de riegos se realizó en base a los canales y parámetros descritos en el manual de la metodología abierta de testeo de seguridad (OSSTMM), mediante la cual se determinó el nivel de riegos al que estaba expuesta la empresa.

- Se seleccionó los controles adecuados de seguridad para realizar un correcto análisis de riesgos de los activos de información e identificar las vulnerabilidades leves o graves a las que están expuestas servidores entes importantes en el desarrollo de las funciones de la empresa.

- Uno de los procesos del análisis de riesgos de los activos de la información es la identificación de los activos más importantes, debido a que si un activo de información importante falla el impacto en la empresa sería grave, sin embargo, dicha apreciación es falsa ya que si un activo menor que presta servicios a otros de nivel superior falla, el daño sería igual o tal vez mayor.

- El análisis de riesgos realizado en la COAC “Escencia Indígena” permitió mitigar, eliminar o transferir el riesgo de las fallas que afectaban el rendimiento de la red; entre las cuales se pudo destacar la inseguridad y mal estado de su cuarto de equipos.

- El manual de políticas de seguridad de la información es el documento más importante en el que se basa la toma de decisiones y acciones a emprender en temas de seguridad, ninguna normativa interna o procedimiento está sobre la política y cualquier violación a la misma deberá ser sancionada conforme al reglamento interno considerando el análisis que si el daño es muy grave se debe adoptar medidas severas.

- Los respaldos de configuraciones e información de equipos informáticos y servidores es primordial de realizar antes de proceder una nueva configuración ya que así se evita pérdida de información y posteriores problemas.

- Se ubicaron los servidores web y mail en una zona desmilitarizada DMZ con el fin de permitir las conexiones tanto desde la red interna como de la externa, mientras que las conexiones que parten de la DMZ solo sean posibles con la red local.

- El equipo gateProtect 500 integra varios servicios de seguridad como es: firewall, DMZ, IDS/IPS además de control de spam, antivirus, proxy y otros lo cual le convierte en una solución integral al momento de proteger una red.

- Mediante el análisis de costos realizado se determinó que utilizar el equipo gateprotect GPA 500 es lo más conveniente para garantizar la estabilidad y continuidad del negocio; ya que este equipo proporciona las mejores características en cuanto aseguramiento de redes perimetrales.

- Después de realizar la comparación entre una solución con software libre y la del equipo GPA 500 se observó que se tiene un mayor ahorro de costos en lo referente a la capacitación, instalación y administración que requiere la solución por software libre.

- Al implementar esta solución la empresa tendrá mayor estabilidad y control de su red; es decir ya no existirá tanta congestión y perdidas de conexión por lo que la atención a sus clientes o socios será más rápida y eficiente que anteriormente lo cual representa un aumento en su productividad y desarrollo empresarial.

- Se realizaron todas las pruebas necesarias para verificar la funcionalidad del firewall y que cada usuario tenga los permisos que le corresponde de acuerdo a su función laboral.

6.3 RECOMENDACIONES

- Es importante documentar los procesos que intervienen en la implementación del SGSI ya que servirá de respaldo y consulta para los funcionarios sepan cómo proceder.

- Se recomienda contratar una persona que se encargue de la seguridad de la red a tiempo completo ya que si se le asigna esta labor al encargado de sistemas, éste no podrá dedicarle la importancia ni el tiempo que se necesita para garantizar dicha seguridad.

- Es necesario definir un método de reporte de incidentes de seguridad que sea amigable con los usuarios que desean reportar fallas, debe incluir información relevante sobre los activos fallidos, agilitando así la solución.

- Se recomienda que todos los funcionarios de la empresa tengan capacitación continua relacionada con la seguridad de la información para evitar incidentes e infiltraciones a los sistemas.

- Se recomienda que al existir dificultades que impidan la implementación de soluciones a riegos y vulnerabilidades encontrados ya sea por falta de apoyo de la dirigencia, recursos económicos, disputas políticas, entre otras, la institución asuma el riesgo y responsabilidad si el activo ocasiona daños a la institución.

- Al instalar un equipo nuevo es necesario realizar el cambio de contraseña a la cuenta de administrador ya que los valores por defecto son conocidos y abren una brecha a personas males intencionados.

- Se debe realizar continuamente pruebas de funcionamiento para determinar fallos en el diseño realizado con el fin de poder corregirlos adecuadamente.

6.4 REFERENCIAS BIBLIOGRAFICAS

DICCIONARIO DE INFORMÁTICA Y TECNOLOGÍA. (2015). *DICCIONARIO DE INFORMÁTICA Y TECNOLOGÍA*. Obtenido de Definición de Fuerza bruta: http://www.alegsa.com.ar/Dic/fuerza%20bruta.php

Castañeda, D. (2013). *Escencia Indígena.*

Erb, M. (2009). *Gestión de Riesgo en la Seguridad Informática*. Obtenido de https://protejete.wordpress.com/gdr_principal/definicion_si/

García, A., Hurtado, C., & Alegre, M. (2011). *Seguridad Informática.* Madrid, España: Paraninfo.

Guijarro, Á. P. (2012). *Seguridad Perimetral*. Obtenido de https://alvaroprimoguijarro.files.wordpress.com/2012/01/ud03_sad_alvaroprimoguijarro.pdf

Herzog, P. (2003). *OSSTMM 2.1.*

Herzog, P. (2003). *OSSTMM 3.0.*

Informática Hoy. (2012). *Informática Hoy*. Obtenido de Seguridad Informática: Qué es Ingenieria Social?: http://www.informatica-hoy.com.ar/software-seguridad-virus-antivirus/Ingenieria-Social-Seguridad-Informatica.php

NTE INEN-ISO/IEC 27002. (2009). *Tecnología de la Información- Técnicas de la Seguridad - Código de Práctica para la Gestión de la Seguridad de la Información.* Quito.

Superintendencia de Economía Popular y Solidaria. (2012). *REGLAMENTO A LA LEY ORGÁNICA DE LA ECONOMIA POPULAR Y SOLIDARIA.*

Toth, G., & Sznek, J. (2014). *Inplementación de la guía NIST SP800-30 mediante la utilizacion de OSSTMM.* Neuquén.

Valdez Alvarado, A. (2013). *OSSTMM3. Analisis y Diseño de Sistemas de Información.*

ÍNDICE DE ACRÓNIMOS

ACL: Access Control List. (Listas de Control de Acceso)

COAC: Cooperativa de Ahorro y crédito

DMZ: Demilitarized Zone (Zona Desmilitarizada)

DNS: Domain Name System (Sistema de Nombres de Dominio)

FTP: File Transfer Protocol (Protocolo de Transferencia de Archivos)

HTTP: Hypertext Transfer Protocol (Protocolo de Transferencia de Hipertexto).

ICMP: Internet Control Message Protocol (Protocolo de Mensajes de Control de Internet)

IDS: Intrusion Detection System (Sistema de detección de intrusiones)

IEC: Comisión Electrotécnica Internacional**.**

IEEE: Institute of Electrical and Electronic Engineers (Instituto de Ingeniería Eléctrica y Electrónica)

INEN: Instituto Ecuatoriano de Normalización

IP: Internet Protocol (Protocolo de Internet)

IPS: Intrusion Prevention System (Sistema de Prevención de Intrusiones)

ISECOM: Federal Information Processing Standard (Estándares Federales de Procesamiento de la Información)

ISO: International Standard Organization (Organización Internacional para la Estandarización)

MAC: Media Access Control (Control de Acceso al Medio)

NIC: Network Interface Card (Tarjeta de Interfaz de Red)

NTE: Norma Técnica Ecuatoriana

OSSTMM: Open Source Security Testing Methodology Manual (Manual de la Metodología Abierta de Testeo de Seguridad)

RAV: Risk Assessment Values (Valores de la Evaluación de Riesgos)

SMTP: Simple Mail Transfer Protocol (Protocolo Simple de Transmisión de Correo)

SSH: Secure SHell.

TCP: Transmission Control Protocol (Protocolo de control de transmisión)

UDP: User Datagram Protocol (Protocolo de Datagrama de Usuario)

UPS: Uninterrupted Power Supply (Sistema de Alimentación Ininterrumpida)

URL: Uniform Resource Identifier (Identificador uniforme de recurso)

VLAN: Virtual Local Area Network (Red de Área Local Virtual)

VPN: Virtual Private Network (Red privada virtual)

ANEXOS

ANEXO 1: HOJA DE DATOS DEL EQUIPO GPA 500

gateprotect®
A Rohde & Schwarz Company

GPA 500 – APLICACIÓN UTM DE ÚLTIMA GENERACIÓN

La aplicación UTM de Última Generación GPA 500 de gateprotect se ha adaptado para las medianas empresas que valoran la fiabilidad, el buen rendimiento y el alto nivel de seguridad. La Gestión Unificada de Amenazas permite una relación de costo-eficiencia y una completa protección combinada con el mejor rendimiento. Gracias a la aplicación de la tecnología eGUI, el GPA 500 puede ser administrado de forma rápida y sencilla. Una multiplicidad de actualizaciones y potentes características de seguridad en el área de antivirus, prevención de intrusiones o control de aplicaciones, ofrecen una protección fiable contra el malware, spam, troyanos, DoS, phishing y otros ataques. La combinación de todos los mecanismos de defensa en un sólo dispositivo hacen que sean innecesarias las inversiones de alto costo en varias soluciones independientes.

Los últimos avances en hardware lo adecuan para el montaje en armarios de servidores, además de que incluye seis interfaces de red que se pueden configurar individualmente. El consiguiente uso de los componentes de servidores de alta calidad en el GPA 500 permite altas velocidades de transferencia superiores a la media, lo que proporciona una integral seguridad UTM combinada con un alto rendimiento.

La conexión de áreas externas a través de VPN, así como la utilización como punto extremo para la conexión con otros lugares puede realizarse sin problemas a través del GPA 500. Gracias a las flexibles posibilidades de aplicación, el buen desempeño y la excelente relación precio-calidad, el GPA 500 es la elección perfecta para las pequeñas y medianas empresas que desean proteger su entorno de red de forma segura pero a un precio favorable.

Security made in Germany

Especificaciones	GPA 500
Interfaces	
Puertos GbE	6xRJ45 (frontal)
Rendimiento del Sistema*	
Rendimiento de Firewall (MBit/s)	2 100
Rendimiento de VPN con IPSec (MBit/s)	320
Rendimiento de UTM (MBit/s)	300
Rendimiento de IPS (MBit/s)	400
Sesiones simultáneas	1 000 000
Nuevas sesiones por segundo	7 000
Dimensiones	
Altura x Ancho x Profundidad (mm)	44 x 426 x 238
Peso bruto (kg)	3
Energía	
Voltaje de entrada (V)	AC 100-240
Consumo de energía totalmente cargado (W)	41 W
Ambiente	
Temperatura de funcionamiento (°C)	0 ~ 40
Temperatura de Almacenamiento (°C)	-10 ~ 70
Humedad Relativa (sin condensación)	20 ~ 90 %

Certificación Hardware

FC CE UL

* El rendimiento del sistema depende del nivel de aplicación y el número de conexiones VPN activas. No ofrecemos una garantía expresa o implícita por la corrección/actualización de la información contenida aquí (la cual se puede modificar en cualquier momento). Los futuros productos o funciones estarán disponibles en el momento adecuado.

gateprotect®
A Rohde & Schwarz Company

gateprotect ha sido proveedor líder a nivel mundial en soluciones de seguridad de TI y en el ámbito de la seguridad de la red durante más de diez años. Estas soluciones comprenden el Firewall UTM de Última Generación con todas las funcionalidades UTM de uso común, seguridad administrada, así como sistemas de cliente VPN.

Empresas e instituciones de buena reputación en más de 80 países alrededor del mundo confían en gateprotect como su socio de seguridad de TI de red. Desde 2010, GateProject ha sido incluido en el famoso „Cuadrante Mágico de Gartner" para las aplicaciones Firewall UTM fi. Para la operatividad fácil y seguridad integral de las soluciones de próxima generación UTM Firewall, gateprotect fue la primera empresa alemana en ser honrado con el Premio a la Excelencia de Frost & Sullivan.

gateprotect es parte del grupo Rohde & Schwarz. El grupo de electrónica Rohde & Schwarz es un proveedor líder de soluciones en los campos de prueba y medida, la radiodifusión, comunicaciones seguras, radiomonitoreo y radiolocalización.

gateprotect GmbH
Valentinskamp 24
20354 Hamburg / Germany

Teléfono línea directa
+49 (0) 40 278 850

Internet
www.gateprotect.com

gateprotect®
A Rohde & Schwarz Company

DESCRIPCIÓN GENERAL DE LAS CARACTERÍSTICAS
APLICACIONES FIREWALL/UTM DE ÚLTIMA GENERACIÓN

Las aplicaciones UTM de Última Generación de gateprotect se caracterizan por una óptima escalabilidad, seguridad y rendimiento.

Gracias a una tecnología eGUI® única y patentada, gateprotect establece estándares cuando se trata de la configuración de los modernos sistemas de seguridad.

La tecnología eGUI® de gateprotect aumenta la seguridad operativa y de eficiencia a un nivel nunca antes alcanzado. Además, es el único fabricante en todo el mundo para implementar la norma ISO 9241. gateprotect fue honrado recientemente con el Premio Mejores Prácticas Frost & Sullivan 2011.

„gateprotect ofrece productos UTM que se destacan entre la competencia debido a su facilidad de uso y efectividad de seguridad. La interfaz de usuario gráfica y ergonómica de gateprotect (eGUI) proporciona la interfaz de gestión visual UTM más intuitiva y eficaz disponible en el mercado".

Frost & Sullivan, Agosto 2011

Especificaciones de las Características

GESTIÓN

- Administración de Firewall basado en roles
- SSH-CLI
- Configuración de escritorio guardada/reestablecida por separado de la copia de seguridad
- Configuración de Firewall orientada a objetos
- Función de actualización de cliente directa

eGUI® technology

Interfaz de usuario gráfica y ergonómica
- Compatible con ISO 9241
- Retroalimentación visual inmediata para cada ajuste
- Funciones autoaclaratorias
- Descripción general de todos los servicios activos
- Descripción inmediata de toda la red
- Función de capa y zoom

AUTENTICACIÓN DEL USUARIO

- Directorio activo/ soporte OpenLDAP
- Base de datos de usuario local
- Autenticación de la interfaz Web
- Autenticación de cliente Windows
- Inicio de sesion única con Kerberos
- Inicio de session única o múltiple
- Web Landing page

CONTROL DE TRÁFICO DE RED/QOS

- Múltiples conexiones de internet modeables por separado
- Todos los servicios modeables por separado
- Ancho de banda ajustable garantizada y máxima
- QoS con soporte TOS-ll ags
- QoS dentro de soporte de conexión VPN

ALTA DISPONIBILIDAD

- HA activo/pasivo
- Sincronización de estado
- Soporte de enlace dedicada multiple y solo
- Conmutación por error por estado

COPIA DE SEGURIDAD Y RECUPERACIÓN

- Archivos de copia de seguridad pequeños
- Restauración y copia de seguridad remota
- Copias de seguridad automáticas y basadas en tiempo
- Carga automática de copias de seguridad en servidor FTP o SCP
- Opción de recuperación de unidad USB

SOPORTE LAN/WAN

- Ethernet 10/100 MBits/s
- Gigabit Ethernet
- MTU cambiable (Ethernet/DSL)
- Autenticación PPP PAP, PPP CHAP
- Tiempo de espera de inactividad/ tiempo de desconexión forzada
- xDSL
- Soporte multi WAN
- Conmutación por error WAN
- Balance de carga
- Conexiones de internet con tiempo Controlado
- Asignación DNS manual y automática
- Soporte dynDNS múltiple
- Enrutamiento basado en la fuente
- Protocolos de enrutamiento RIP, OSPF
- DHCP
- DMZ

VLAN
- 4094 VLAN por interfaz
- Etiquetado de encabezado 802.1q ethernet
- Combinable con puente

Modo Puente
- Función Firewall OSI-Layer 2
- Árbol de expansión (bride-ID, port-cost)
- Interfaces ilimitadas por puente
- Combinable con VPN-SSL

REGISTROS, INFORMES, ESTADÍSTICAS

- Informes de correos electrónicos
- Inicio de sesión para varios servidores syslog
- Inicio de sesión en admin-cliente (con filtro)
- Exportación a archivos CSV
- Estadísticas de grupo IP e IP
- Servicios por separado
- Usuario único/grupos
- Listas Top (surfcontrol)
- Estadísticas de tráfico/IDS
- Estadísticas de Tráfico de Control de Aplicaciones
- Estadísticas Antispam/antivirus
- Estadísticas de defensa

MONITOREO

- Información del Sistema (CPU,HDD,RAM)
- Red (Interfaces, enrutamiento, tráfico, errores)
- Procesos
- VPN
- Autenticación de usuario

SNMP
- SNMPv2C
- SNMP-trampas
- HA*

GESTIÓN UNIFICADA DE AMENAZAS

Filtro Web
- Filtro de URL con aplicación de búsqueda segura
- Filtro de contenido
- Reglas de bloqueo para nivel de usuario
- Listas Blanca/negra
- Importación/Exportación de listas URL
- Bloqueo de extension de archivos
- Bloqueo de sitio web basado en categorías
- Categorías auto definidas
- Tecnología de exploración con base de datos en línea
- Soporte proxy HTTP-no transparente

Control de aplicaciones
- Filtrado de paquetes capa 7 (DPI)
- Filtrado de aplicaciones en lugar de puertos
- Detección y Control de Skype, Bittorrent y otros, así como también aplicaciones de Web 2.0 como Facebook

Antivirus
- Kaspersky Anti-Virus Engine
- Completa Protección de todos los programas maliciosos
- HTTP, HTTPS
- FTP, POP3, SMTP
- Excepciones definibles
- Actualizaciones automáticas y manuales

Antispam
- Nivel de escaneo ajustable
- Detección de Spam en tiempo real
- Nube GlobalView utilizando Detección de Patrones Recurrentes (RPD)
- Filtrado de correo
- Listas blanca/negra
- Rechazo/eliminación automática de correos electrónicos
- Importación de Dirección de correo electrónico AD

Prevención de Intrusiones
- Reglas individuales personalizadas
- Nivel de seguridad ajustable
- Grupos de reglas seleccionables
- Excepciones definibles
- Análisis de todas las interfaces
- Protección de Puerto scan, DoS
- Protección de paquetes de redes maliciosas

Proxies
- HTTP (transparente o no transparente)
- HTTPS
- Soporte para el servidor Radius, servidor AD, base de datos de usuario local
- FTP, POP3, SMTP, SIP
- Controlada por tiempo

VPN

- Asistente VPN
- Asistente de Certificado
- Sitio a Sitio
- Cliente a Sitio (Road Warrior)
- PPTP
- Exportación a conexión de un click

Certificados X.509
- CRL
- OCSP
- Soporte CA multiple
- Suporte Host Cert multiple

IPSec
- Modo tunel
- IKEv1, IKEv2
- PSK/ Certificados
- DPD (Detección de Extremo Muerto)
- NAT-T
- XAUTH, L2TP

SSL
- Modo de enrutamiento VPN
- Modo de Puente VPN
- TCP/UDP
- Servidores DNS y WINS específicos

CENTRO DE COMANDO

- Monitor y configuración active de Firewalls 500+
- Configuración central y Monitoreo de conexiones VPN
- Copia de seguridad individual y grupal
- Plan de copia de seguridad automático en grupos
- Licencia y actualización grupal e individual
- Creación de plantillas de configuración y aplicadas en multiples firewalls
- Autoridad de Certificado
- Certificado en base a conexiones cifradas 4096 bit a los firewalls
- Visualización de la configuración de todos los firewalls
- Gestión de usuario basado en roles.

SC MAGAZINE RECOMMENDED

SecurITy made in Germa

ANEXO 2: PROFORMA EQUIPO GATEPROTECT GPA 500

PROPUESTA DE FIREWALL

GATEPROTECT GPA500

Coop. Escencia Indígena

22 SEPTIEMBRE 2015

SMART HELP SOLUCIONES

Somos una compañía dedicada a brindar soluciones informáticas integrales con los más altos estándares de servicio y calidad. Contamos con experimentado equipo de profesionales en diferentes áreas de la tecnología lo que nos permite brindar soluciones integrales y de gran calidad. Somos integradores de los mejores productos y servicios tecnológicos del mercado con el objetivo de satisfacer de forma integral las necesidades de nuestros Clientes.

Misión

Ser un socio estratégico que brinde soluciones tecnológicas de gran calidad a sus Clientes con un experimentado recurso humano, herramientas innovadoras y altos niveles de seguridad. A fin de satisfacer las necesidades de organización, administración, soporte y mantenimiento tecnológico de nuestros Clientes.

Visión

Ser la Empresa pionera y líder en la provisión de soluciones de gestión y seguridad tecnológica con mejores estándares de calidad y satisfacción al Cliente en el mercado para el año 2016; siendo reconocidos como una empresa que presta servicios de gran valor agregado y alta calidad.

Principios Corporativos

Nuestros Clientes son nuestra mayor prioridad, de este modo estudiamos y analizamos la estructura informática de las empresas para brindarle soluciones óptimas a todas sus necesidades tecnológicas, haciéndole ahorrar tiempo y dinero.

1. NUESTRAS SOLUCIONES

Gracias a la amplia experiencia de nuestros expertos brindamos excelentes soluciones informáticas y respuestas efectivas a los nuevos requerimientos y desafíos de nuestros Clientes. Todas nuestras soluciones tienen como objetivo reducir los costos de gestión y administración tecnológica y aumentar considerablemente la eficiencia de su negocio.

1.1. Consultoría

Gracias a la extensa trayectoria de nuestros consultores de TI brindamos asesoramiento y auditorías en todas las áreas de tecnología de las empresas. Permitiéndoles resolver problemas y planificar de forma adecuada su inversión tecnológica con el objetivo de optimizar recursos y mejorar considerablemente el rendimiento. Además del asesoramiento a nivel técnico, brindamos asesoramiento en planificación estratégica de TI, implementación de estándares ITIL y COBIT.

1.2. Soporte de Infraestructuras

Nuestro multidisciplinario equipo de trabajo estudia las necesidades tecnológicas de nuestros Clientes, cuidando todos los detalles de su infraestructura para brindarle soluciones de implementación y soporte de redes corporativas, servidores de misión crítica, directorio activo, seguridad de la información, entre otros.

1.3. Mesas de Servicios – Service Tonic

Smart Help Soluciones ha sido escogido por Service Tonic como distribuidor exclusivo en Ecuador por su amplia experiencia en la implementación de soluciones de Service Desk.

Service Tonic es un potente software para automatizar y gestionar servicios, mesas de ayuda y gestión de incidencias en un esquema totalmente web, muy fácil de personalizar y administrar. Es totalmente versátil y multi servicio cumpliendo de esta forma con todos los requerimientos de nuestros Clientes.

1.4. Seguridad Informática

Somos integradores de una gran cantidad de soluciones de seguridad informática que le permite a su Empresa contar con toda la protección que su Negocio requiere. Somos proveedores de sistemas de seguridad para redes, servidores y estaciones. Nuestro experimentado equipo de consultores diseña e implementa soluciones robustas y ajustadas a su presupuesto. Distribuimos e implementamos soluciones de Firewall, Antimalware, Monitoreo de seguridades, Aseguramiento de servidores y Ethical Hacking.

1.5. Respaldo y Recuperación de Desastres

Smart Help Soluciones asesora, implementa y asegura los entornos IT, permitiendo a los Clientes poder respaldar y salvaguardar sus datos críticos y así proteger su activo más importante, la información. Con soluciones flexibles, que se ajustan a los requerimientos de nuestros Clientes y que aportan eficiencia en el control y respaldo de su información. Brindamos a nuestros Clientes todo el asesoramiento sobre buenas prácticas para la seguridad de su información, y una amplia gama de soluciones tanto locales como en la nube.

1.6. Soluciones de Cableado Estructurado

Contamos con personal especializado en diseño e instalación de proyectos de infraestructura para redes, cableado estructurado y enlaces inalámbricos. Contamos con productos certificados y garantizados para la implementación de soluciones convergentes de comunicaciones de datos, voz y video.

1.7. Soluciones de Virtualización

Nuestra amplia experiencia y compromiso con la innovación nos ha permitido convertirnos en uno de los principales distribuidores a nivel nacional de sistemas de virtualización tanto a nivel de infraestructura, sistemas operativos y estaciones de trabajo. Las soluciones de virtualización le ofrecen respuestas eficientes a los constantes cambios tecnológicos y le permiten a su empresa reducir significativamente costos de inversión y de administración tecnológicos.

2. Introducción

Smart Help Soluciones S.A. agradece a la **Coop. Escencia Indígena**. Por la oportunidad que nos ha brindado para ofrecer nuestros productos y servicios enfocados en incrementar la seguridad de la información de su Institución.

3. Antecedentes del Proyecto

Coop. Escencia Indígena, requiere de una solución de seguridad de la información a nivel de su red local y perimetral que le permita gestionar de forma eficiente y confiable el acceso a sus recursos informáticos, enfocados en asegurar el entorno tecnológico, controlar servicios de navegación, facilitar la implementación de nuevos servicios a futuro.

4. Presentación del Producto

gateProtect Aktiengesellschaft Germany es un fabricante líder de soluciones de seguridad IT en la gama de seguridad de redes. Su especialidad son las aplicaciones xUTM, productos de cortafuegos y sistemas de encriptación de clientes

Las soluciones de gateProtect combinan prestaciones modernas de seguridad y redes, como cortafuegos, bridging, VLAN, single sign-on, catalogación de tráfico, QoS, IPSec/SSL (X.509), IDS / IPS, filtro de web, filtro de virus, detección de correo basura en tiempo real y proxy HTTPs en un solo sistema.

Lo que hace especiales todos los productos de gateProtect, además de sus prestaciones técnicas, es la administración ergonómica única de los sistemas.

gateProtect es el único fabricante del mundo que implementa las líneas maestras del estándar ISO 9241.

Con su tecnología única y patentada eGUI® (ergonomic Graphic User Interface, o Interfaz Gráfica de Usuario ergonómica) y el nuevo Centro de Control, gateProtect ha posibilitado un gigantesco avance en la configuración y administración de sistemas de cortafuegos. La nueva tecnología eGUI® aumenta la seguridad IT efectiva de las empresas y, al mismo tiempo, aumenta la eficiencia en el mantenimiento de rutina de los sistemas. Esto implica un ahorro significativo en el coste operativo para nuestros clientes.

IT Security made in Germany

gateProtect es miembro fundador de ""IT Security made in Germany" (ITSMIG.e.v.), que cuenta con el apoyo del Ministerio Federal de Economía y Tecnología. La iniciativa ""IT Security made in Germany"" es una asociación de empresas alemanas de seguridad IT que cuenta con el apoyo del Ministerio Federal de Economía y Tecnología. Otros miembros son empresas conocidas como Siemens, Avira, Utimaco, Genua, gateProtect y otras. La intención de la iniciativa es expandir el

conocimiento de las empresas alemanas de seguridad IT y la cooperación entre los miembros de la iniciativa y socios en países extranjeros. La iniciativa cuenta con el apoyo del Ministerio Federal de Economía y Tecnología (BMWi) y funciona como una Asociación Pública-Privada (PPP). El Instituto Fraunhofer de Tecnología de la Información Segura SIT es responsable de la organización y gestión de las redes.

Asistencia con Orientación Sistemática Hacia el Usuario

Gracias a la tecnología eGUI®, gateProtect tiene un 90% menos de necesidad de asistencia que los productos de la competencia. Por ello, gateProtect puede asegurar una asistencia de calidad sin igual en el mercado. La asistencia es proporcionada directamente por los propios trabajadores de gateProtect. Para ello, administradores de redes altamente cualificados y constantemente formados están disponibles para nuestros clientes en todo momento. Solo así se puede garantizar una alta calidad de asistencia. El servicio de asistencia al cliente estará disponible telefónicamente, dependiendo de la validez del contrato de mantenimiento, 7 días a la semana, 24 horas al día con tiempos de respuesta de 0-2 horas (24/7).

5. GPA 500

La gama de modelos GPA 500 está diseñada para empresas de gran tamaño, de hasta 130 equipos y que requieren gran cantidad de conexiones VPN.

Las "aplicaciones de nueva generación UTM"" de gateprotect se caracterizan por una excelente escalabilidad, seguridad y rendimiento. Gracias a una tecnología eGUI"® única y patentada, gateprotect marca estándares en lo que a la configuración de sistemas de seguridad modernos se refiere.

La tecnología eGUI® de gateprotect eleva la seguridad y eficiencia operativas a un nivel nunca antes alcanzado. Además, gateprotect es el único fabricante en todo el mundo en implementar el estándar NORMA ISO 9241.

Las aplicaciones UTM de próxima generación de GPA 500 presentan amplias prestaciones, entre ellas VLAN, tecnología de 8 capas, single sign-on, bridging, VPN SSL a través de certificados x.509 & VPN IPSec, IDS/ IPS, catalogación de tráfico, antivirus, protección hora cero de correo electrónico, filtrado web y la última tecnología eGUI® orientada al proceso. El rendimiento de la conexión VPN se ve marcadamente reforzado por el chip acelerador especial ASIC Crypto.

5.1. Ventajas de la Tecnología de 8 capas

5.1.1. Control de la política de seguridad basada en el usuario

La "tecnología de 8 capas"" de gateprotect trata la identidad del usuario como la octava capa del modelo OSI."

"Todas las ""aplicaciones UTM de nueva generación"" de gateprotect ofrecen seguridad y productividad a todos los niveles y en todos los servicios, desde la capa 2 a la capa 8 con políticas basadas en la identidad."

5.1.2. A prueba de futuros cambios con alta seguridad

La mayoría de los sistemas modernos de cortafuegos admiten autentificación de usuarios basada en proxy. Esto significa que solo los servicios que funcionan con proxies, como HTTP o FTP, pueden ser otorgados a usuarios específicos.

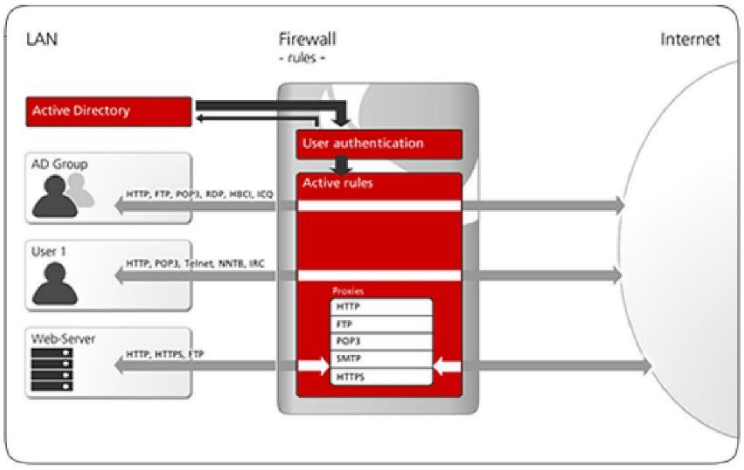
El cortafuegos de gateprotect tiene una Autentificación Extendida de Usuario que permite que un número cualquiera de servicios se asignen a un usuario o un grupo de usuarios. Estos servicios pueden proporcionarse con todas las opciones adicionales conocidas, como proxies o filtros web.

Si un usuario inicia sesión en el cortafuegos desde un ordenador, todos los servicios asignados al ordenador en cuestión están habilitados.

5.1.3. Gateprotect le ofrece dos maneras de iniciar sesión en el cortafuegos:

Navegador web/Cliente UA: el inicio de sesión se realiza mediante conexión HTTPS.

Single sign-on: Kerberos automáticamente transfiere el inicio de sesión en el dominio al cortafuegos.



5.1.4. La autentificación de usuario extendida de gateprotect convence por

- La asignación de tantos servicios como se desee a una persona
- Configuración de los servicios para grupos
- Configuración de los servicios para grupos de Active Directory
- Aprobación de servicios también en la Intranet

- Futuro garantizado, porque los futuros servicios también serán configurables.
  Single sign-on con Kerberos durante el registro en el dominio de Windows
- Inicio de sesión en el navegador para interdependencia operativa del sistema

6. Propuesta de Implementación

Gracias a nuestra amplia experiencia en la implementación de soluciones de seguridad y networking sugerimos a su Institución seguir el siguiente plan de implementación que nuestra empresa ofrece:

- ✓ Análisis de la infraestructura actual.
- ✓ Definición de alcance u objetivos a ser cumplidos con la implementación del nuevo equipo de seguridad.
- ✓ Diseño de implementación, en el que se establece la nueva estructura de la red una vez que se implemente el nuevo equipo de seguridad.
- ✓ Evaluación de impacto y cambios sobre la red que tendrá la implementación del nuevo equipo de seguridad.
- ✓ Documentación de diseño y análisis.
- ✓ Configuración inicial del equipo de acuerdo al diseño.
- ✓ Prueba de implementación del equipo.
- ✓ Paso a producción del nuevo equipo de seguridad.
- ✓ Pruebas y corrección de errores. ✓ Monitoreo periódico del equipo.

7. Propuesta Económica

7.1. Licenciamiento a 1 Año

Producto	Cantidad	Precio
Valores a cancelar		
1. Firewall GateProtect GPA500 + UTM Apliance • Interface 100% gráfica (eGUI) con funcionalidad "Drag & Drop". • Firewall. • LAN / WAN-support. • User authentication. □ DHCP. • DMZ • VLAN. • Bridge-mode. • Traffic shaping. • Proxies. • Antivirus. • Web-filter. • Antispam. • High availability. • IDS/IPS • Statistics. • VPN. • Logging, Reporting. • Solución IPSec y SSL sitio-a-sitio con certificados X.509. • GARANTIA EQUIPO 2 AÑOS	1	$2,100.00
2. Suscripción Premium por un Año Esto incluye: Actualizaciones y soporte por un año. **Paquete UTM** • GPA-500 - Spam- Filter (por 12 meses). • GPA-500 - Web- Filter (por 12 meses). • GPA 500 – Aplication Filter (por 12 meses). • GPA-500 - Virus- Filter (por 12 meses).	1	$1500.00
3. Servicio de diseño y Pre implementación Servicios descritos en el numeral 6 de la presente propuesta.	1	$500.00
TOTAL A PAGAR		**$4,100.00**

8. Condiciones Comerciales

Para cualquier de las ofertas que constan en el presente documento, aplican las siguientes condiciones comerciales:

- Los precios que constan en la tabla anterior no incluyen el IVA, el cual se debe añadir a los valores expresados.

- Los precios que constan en la tabla anterior se encuentran expresados en dólares de los Estados Unidos de Norteamérica.

9. Forma de Pago

Nos permitimos proponer la siguiente forma de pago de los productos ofertados:

- A la aceptación de la presente propuesta se cancelará el 60% inicial del monto total del equipo GateProtect, la Suscripción Premium, Paquete UTM y los servicios de diseño e implementación.
- Una vez que se haya instalado y configurado el Firewall a satisfacción de su Institución, se cancelará el 40% restante.

Esperamos que los productos y servicios presentados sean de su interés y cubran las necesidades de su Institución. Cualquier inquietud no duden en contactarnos que estaremos gustosos de satisfacerla.

Atentamente,

Patricio Starnfeld
Gerente General
Smart Help Soluciones S.A.

ANEXO 3: COMPROBANTE DE EXISTENCIA LEGAL

Fecha de Generación de Documento: 23/febrero/2016

Validez de Documento: 30 días a partir de la fecha de generación

COMPROBANTE DE EXISTENCIA LEGAL DE ORGANIZACIONES DE LA ECONOMÍA POPULAR Y SOLIDARIA

Revisado el Catastro Digital de Organizaciones de esta Superintendencia, consta la siguiente información de la COOPERATIVA DE AHORRO Y CREDITO ESCENCIA INDIGENA LTDA

DATOS DE LA ORGANIZACIÓN

No. RESOLUCIÓN CONSTITUCIÓN/ADECUACIÓN: SEPS-ROEPS-2013-000355
FECHA DE RESOLUCIÓN CONSTITUCIÓN/ADECUACIÓN: 04/22/2013

RUC:	1091722425001
SECTOR:	COOP-SFPS
RAZÓN SOCIAL:	COOPERATIVA DE AHORRO Y CREDITO ESCENCIA INDIGENA LTDA
PROVINCIA:	TUNGURAHUA
CANTÓN:	AMBATO
PARROQUIA:	MATRIZ
SEGMENTO / NIVEL:	SEGMENTO 3
ESTADO:	ACTIVA

La información constante en el presente documento, corresponde a la recibida de la organización, quien asume cualquier tipo de responsabilidad por error o falsedad de la misma. En caso de querer validar ésta información deberá ingresar en la página web: www.seps.gob.ec

El presente comprobante carecerá de validez probatoria en un proceso judicial; para el efecto, se solicitará la respectiva certificación.

SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA

ANEXO 4: INSTALACIÓN DEL SERVIDOR FIREWALL CON VMWARE

Con VMware (Estación de trabajo, Servidor-ESX) es posible montar la imagen ISO que se utilice para quemar el CD. Se puede proceder de manera normal con la instalación.

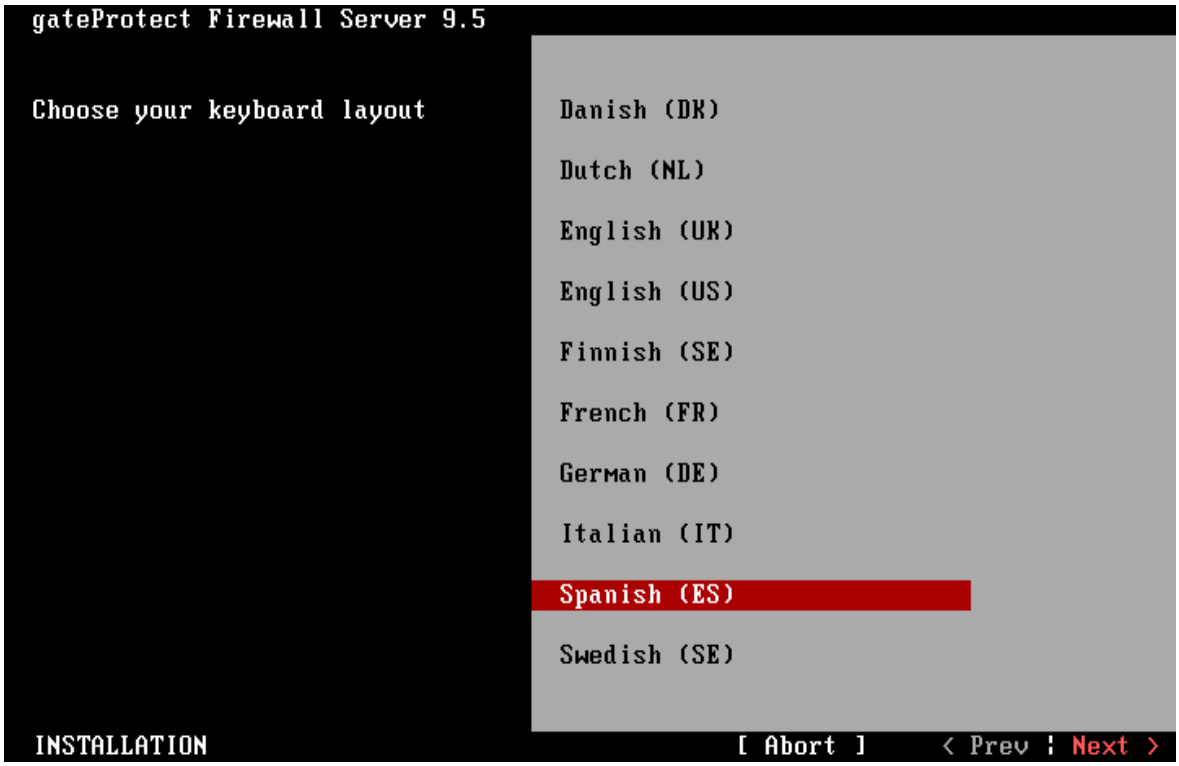
Requisitos del hardware para la máquina virtual:

HDD: 20 GB

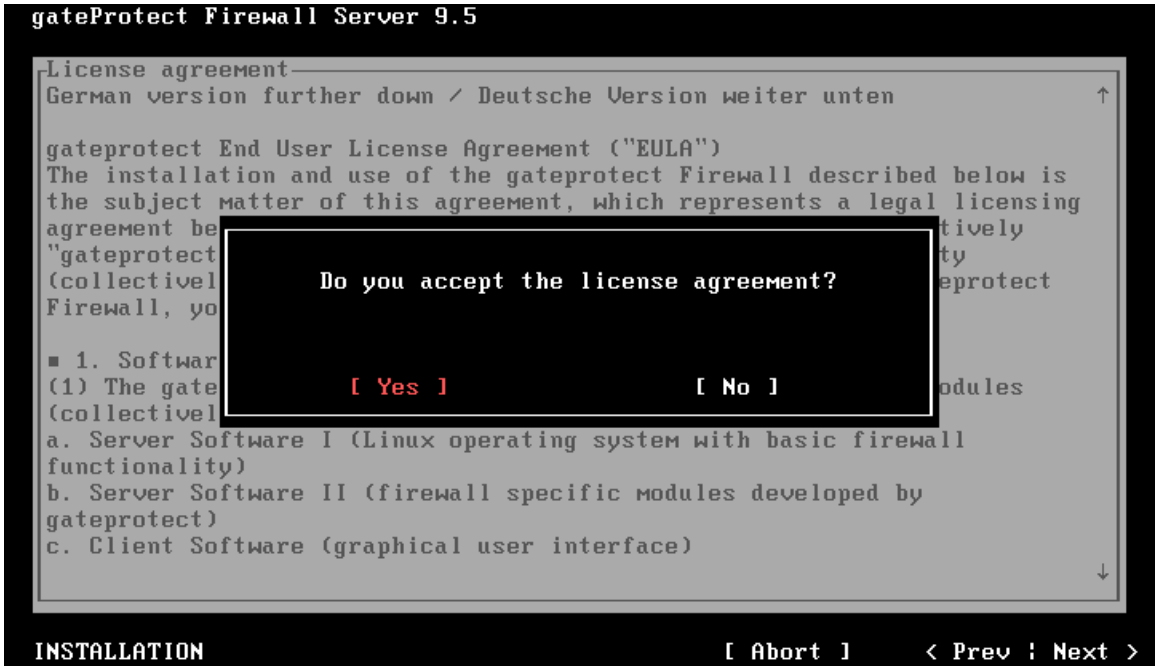
RAM: 1GB

Estos requerimientos deben ser adaptados al objetivo que se espera lograr y al número de usuarios.

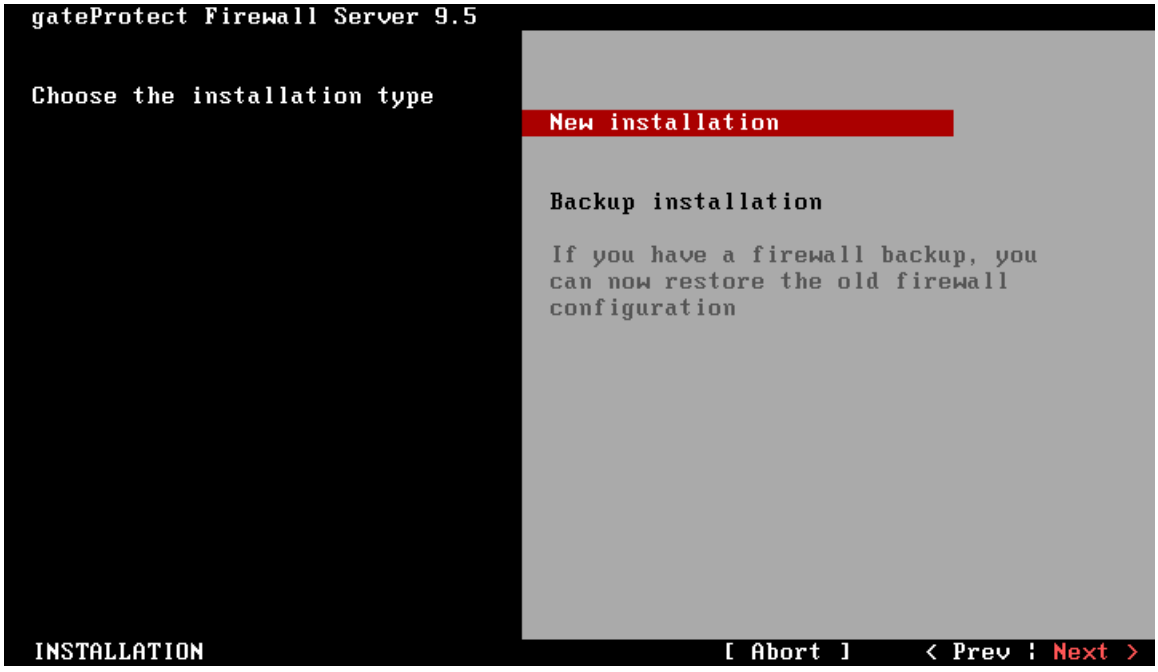
1. Inserte el CD-Instalación en el CD-drive del VMware-PC e inicie la máquina virtual. Elegir el idioma y seleccionar Next.



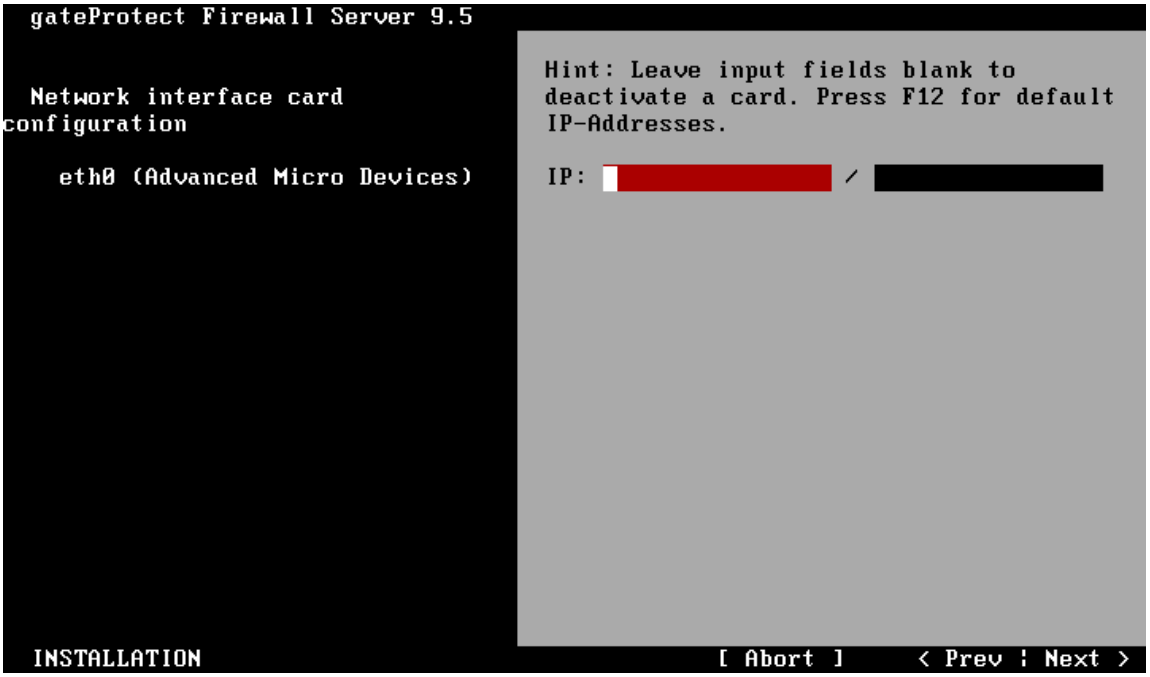
2. Aceptar los términos de la licencia seleccionando la opción Yes y continuar.



3. Seleccionar el tipo de instalación- New installation

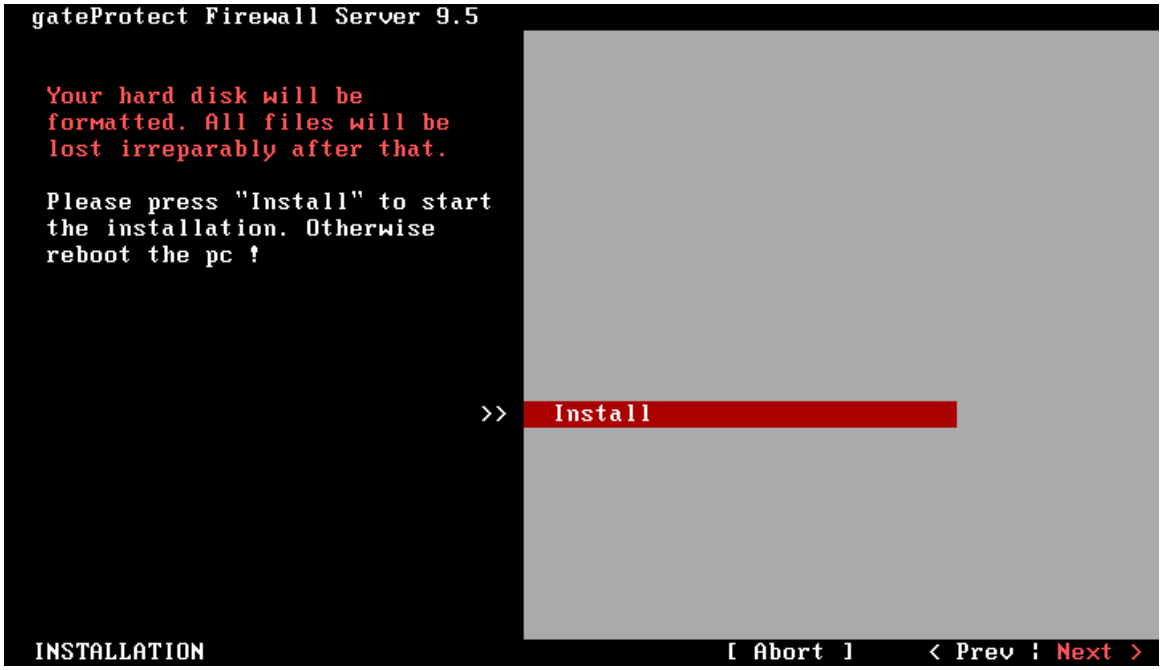


4. Instalar los dispositivos de red, asignar a cada tarjeta una ip y una máscara de red asociada.



5. Ingresar el nombre, dominio y contraseña para el servidor. Se recomienda elegir una contraseña de al menos 8 digitos.

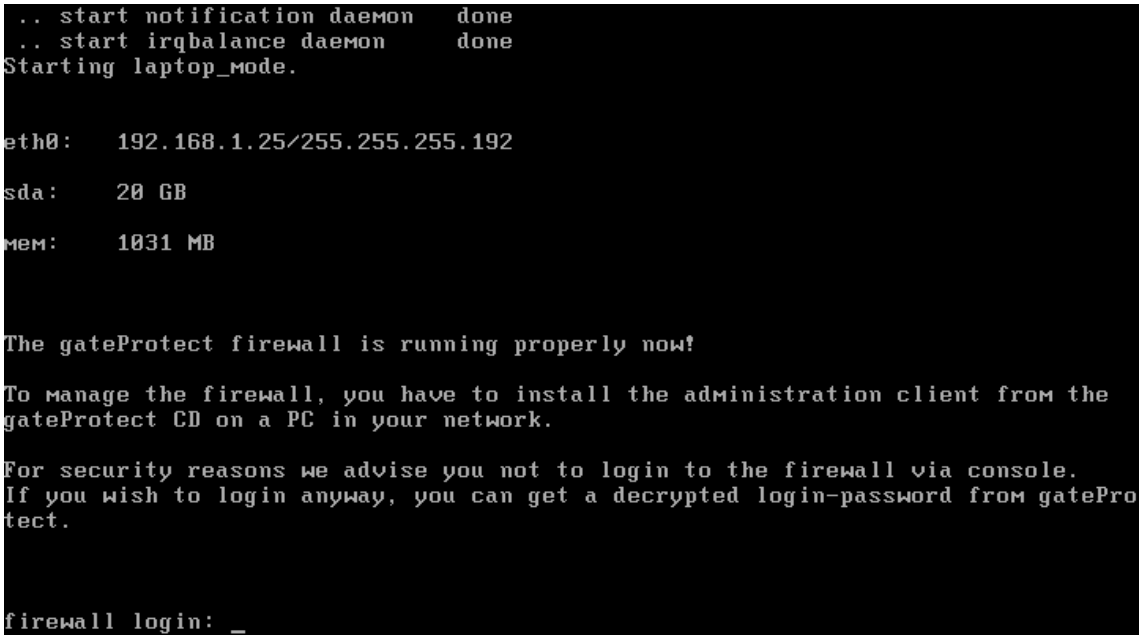
6. Seleccionar la opción Instalar.



7. La siguiente pantalla informa que el disco seleccionado será formateado. Presionar en Yes para continuar.

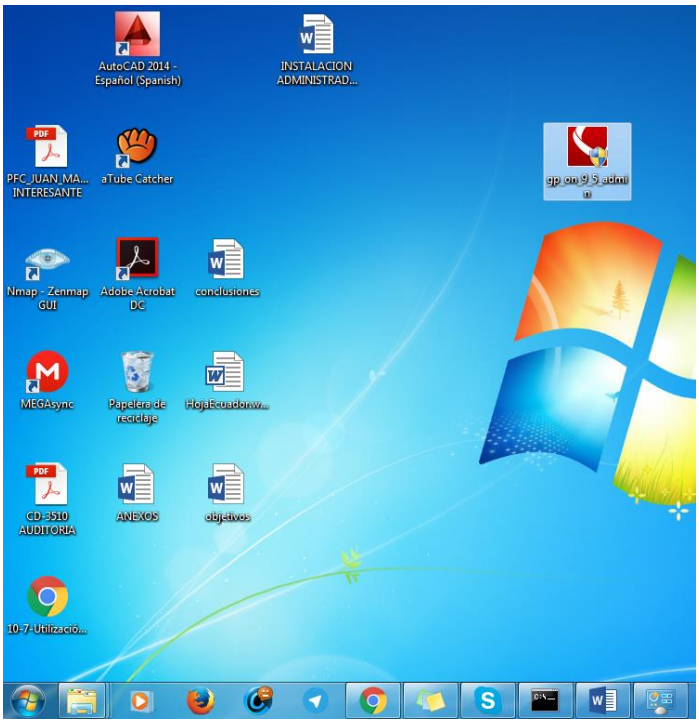
8. Si la instalación se realiza correctamente se mostrará la siguiente pantalla.

9. Al finalizar mostrará la pantalla mostrada la cual indica que el servidor está listo para ser administrado.

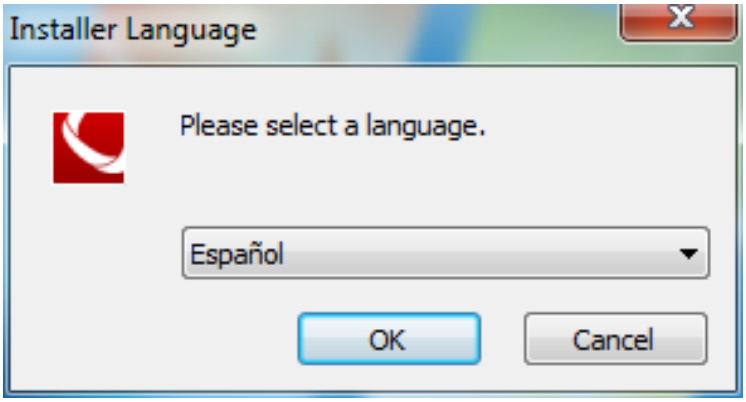


ANEXO 5: INSTALACIÓN DEL CLIENTE DE ADMINISTRACIÓN.

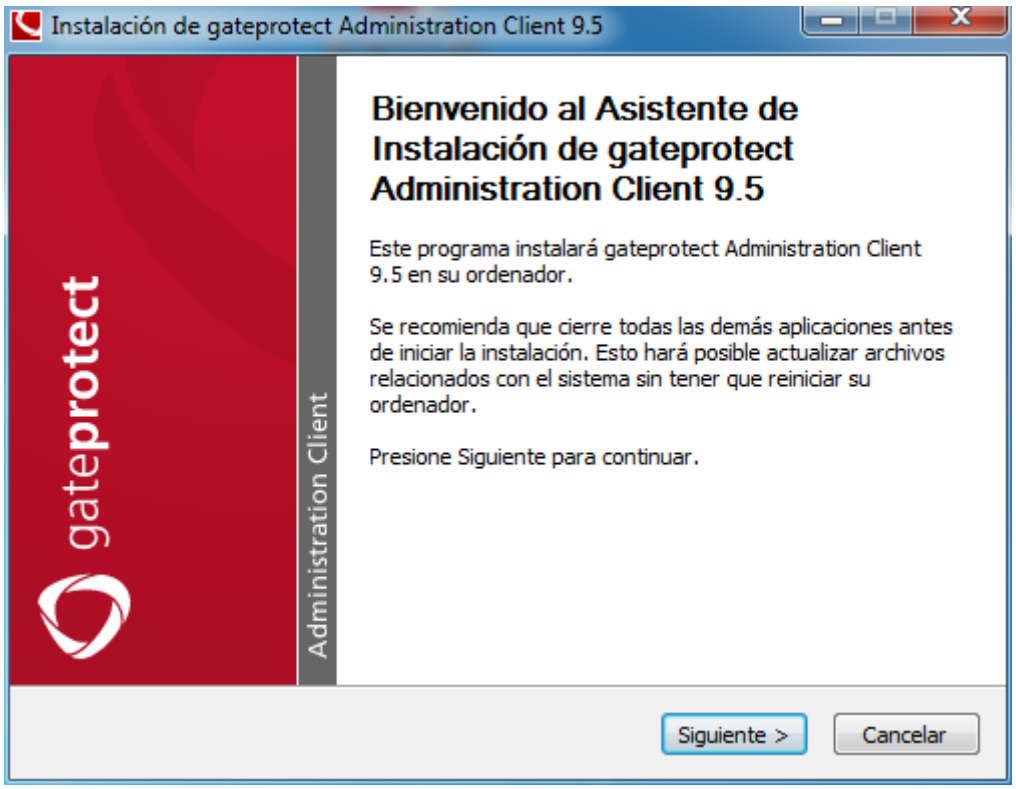
1. Ejecutamos el instalador presionando click derecho y eleigiendo la opción ejecutar como administrador.



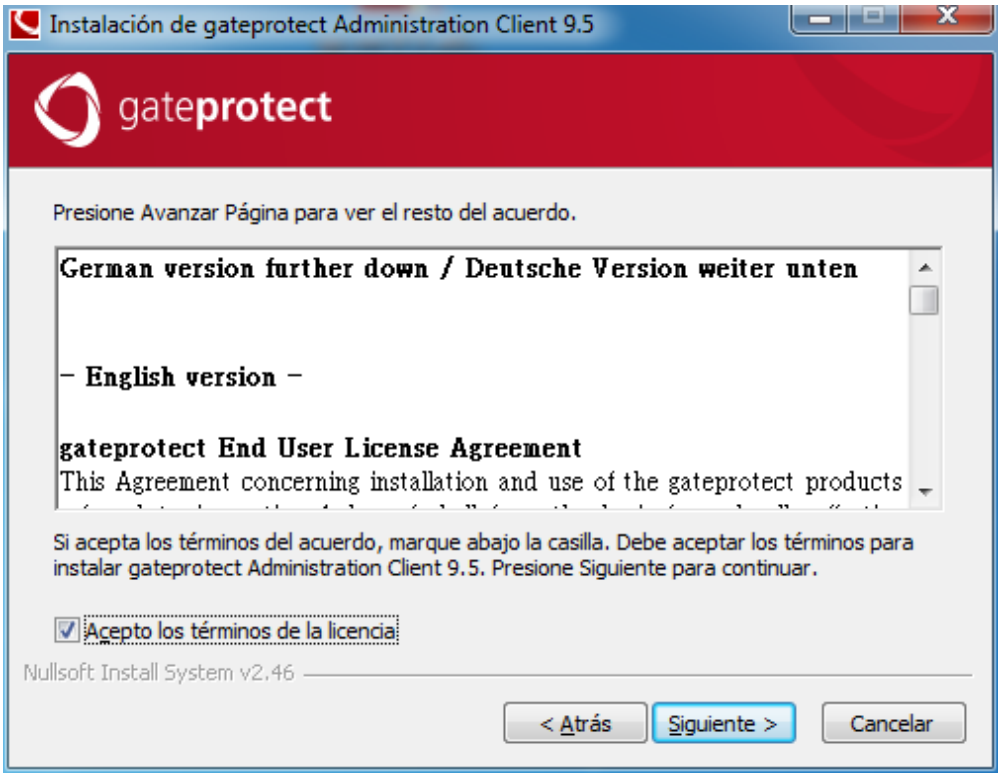
2. Seleccionar el idioma de instalación y presionar Ok para continuar



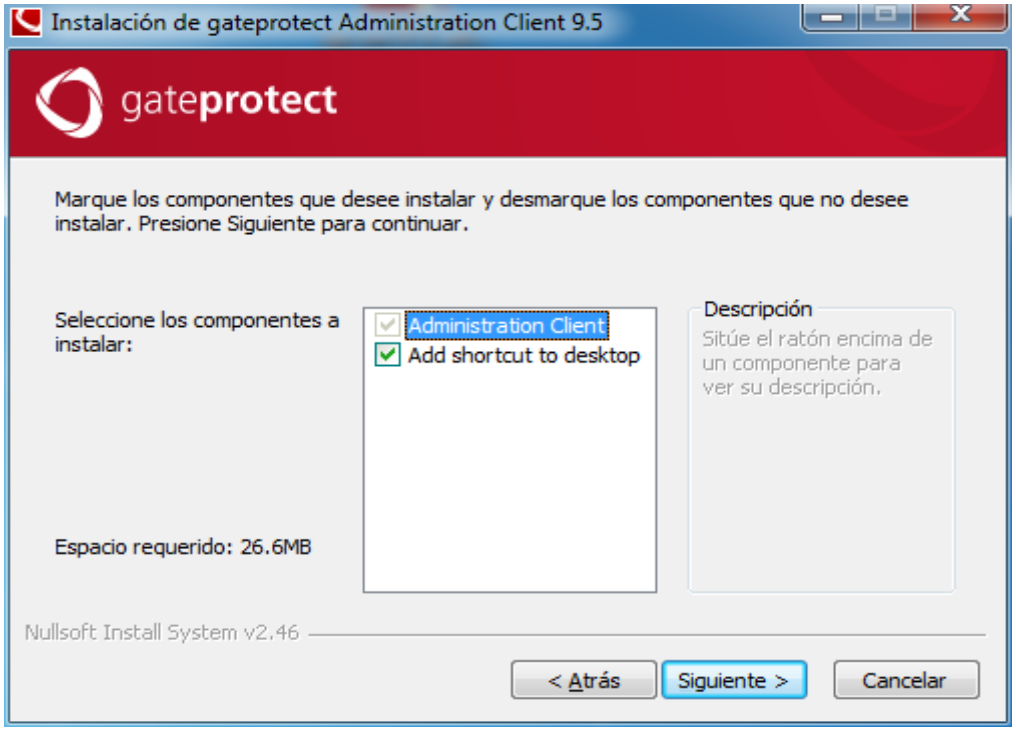
3. Se abre el asistente de instalación, presionar siguiente para continuar.



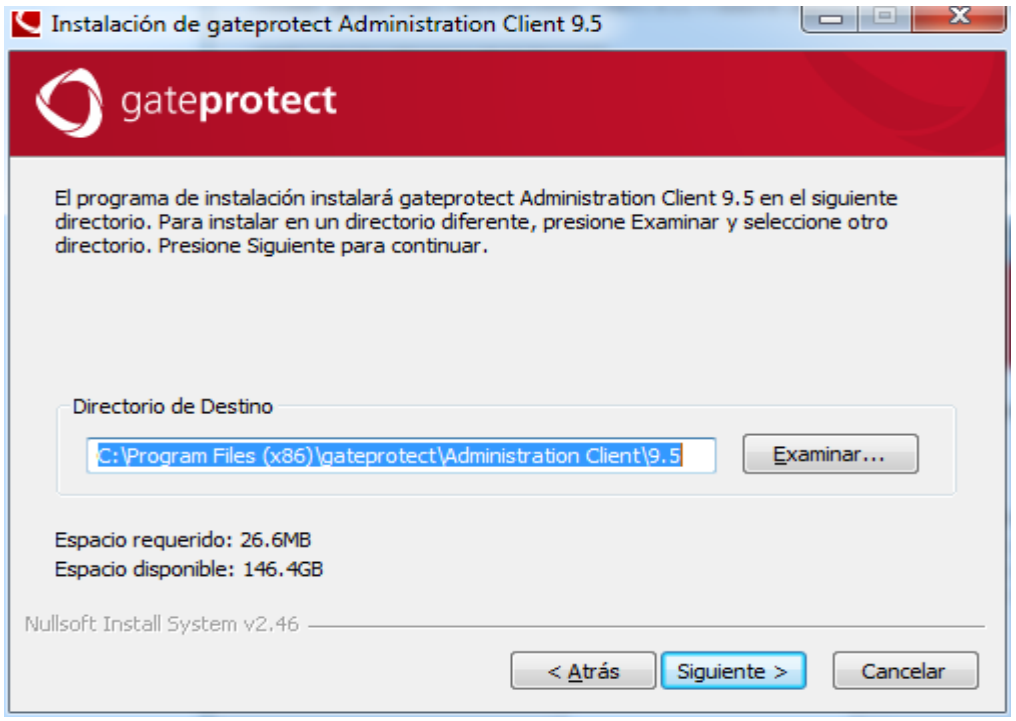
4. Aceptar los términos de la licencia y presionar siguiente.



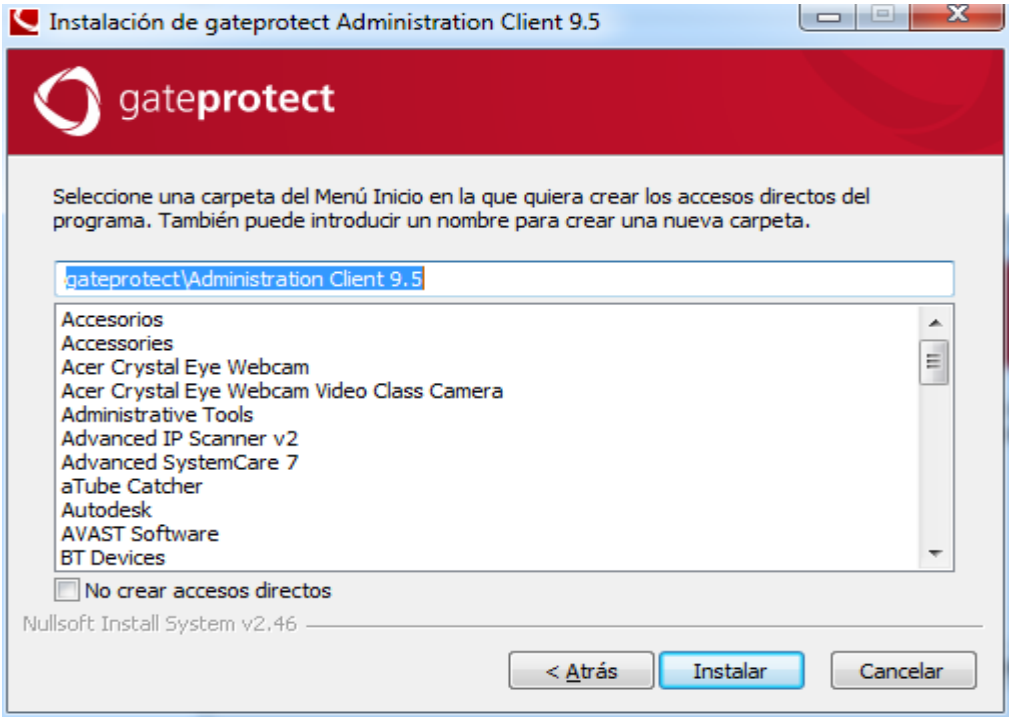
5. En la siguiente pantalla mantener los datos como se muestra y presionar siguiente.



6. La siguiente ventana muestra la dirección en la cual se instalará el software, presionar en siguiente.



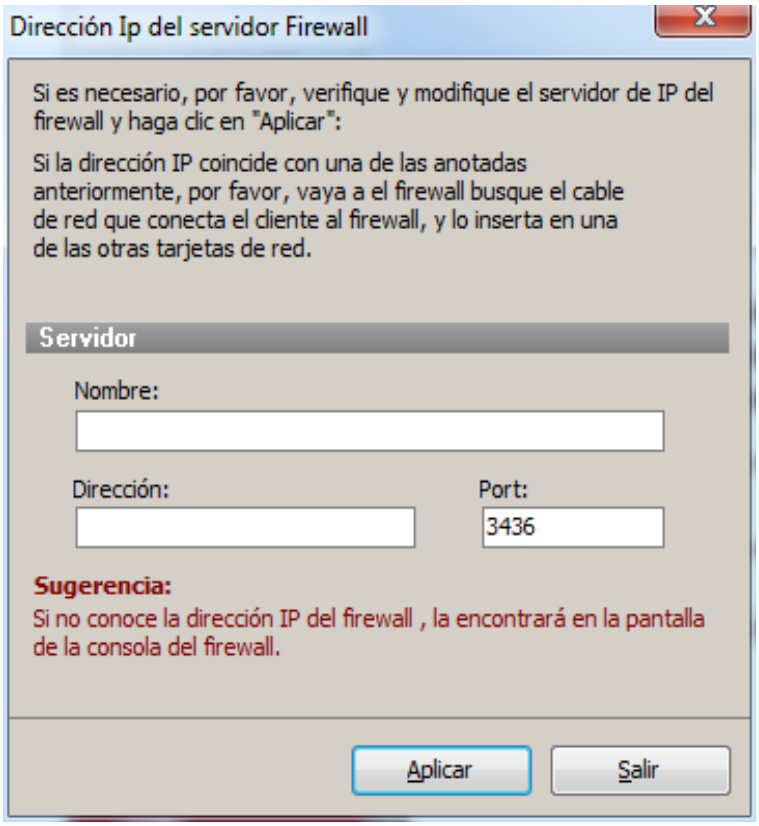
7. A continuación elegir la carpeta en la cual se crearán los íconos de acceso directo, presionar en siguiente.



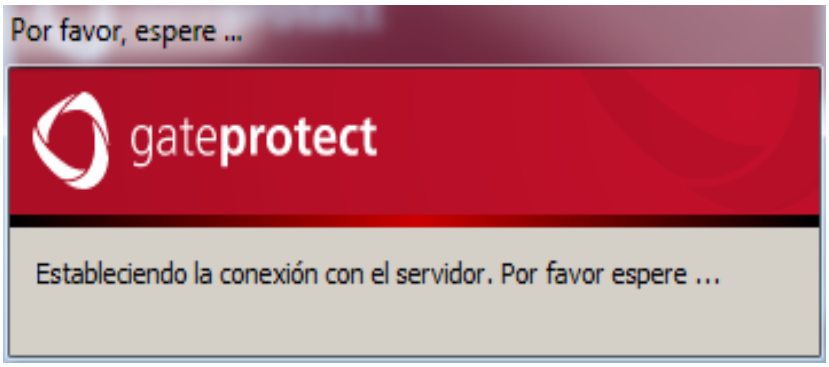
8. Click en Terminar para completar la instalación.

CONFIGURACIÓN E INICIO DEL ASISTENTE

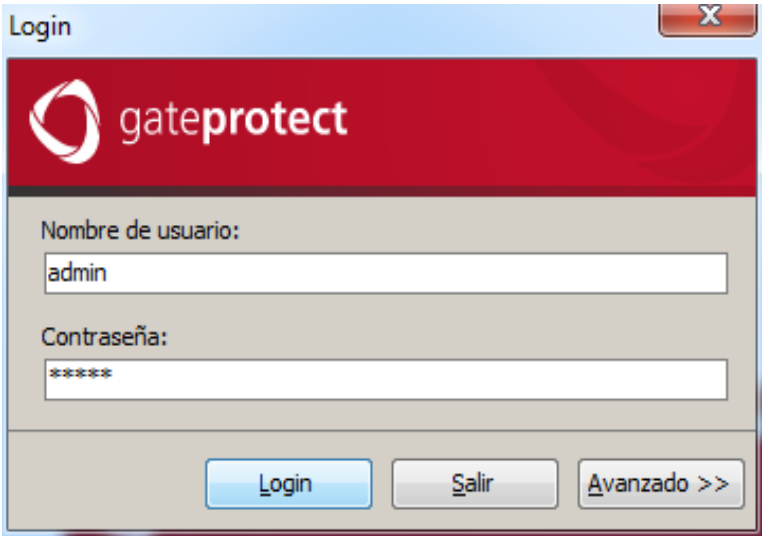
1. Ejecutar el icono de acceso directo del asistente. Al abrirse muestra la siguiente ventana en la cual ingresamos el nombre y dirección Ip del servidor firewall.



2. Si se han ingresado correctamente los datos anteriores aparecerá la siguiente ventana que indica que se está conectando con el servidor.



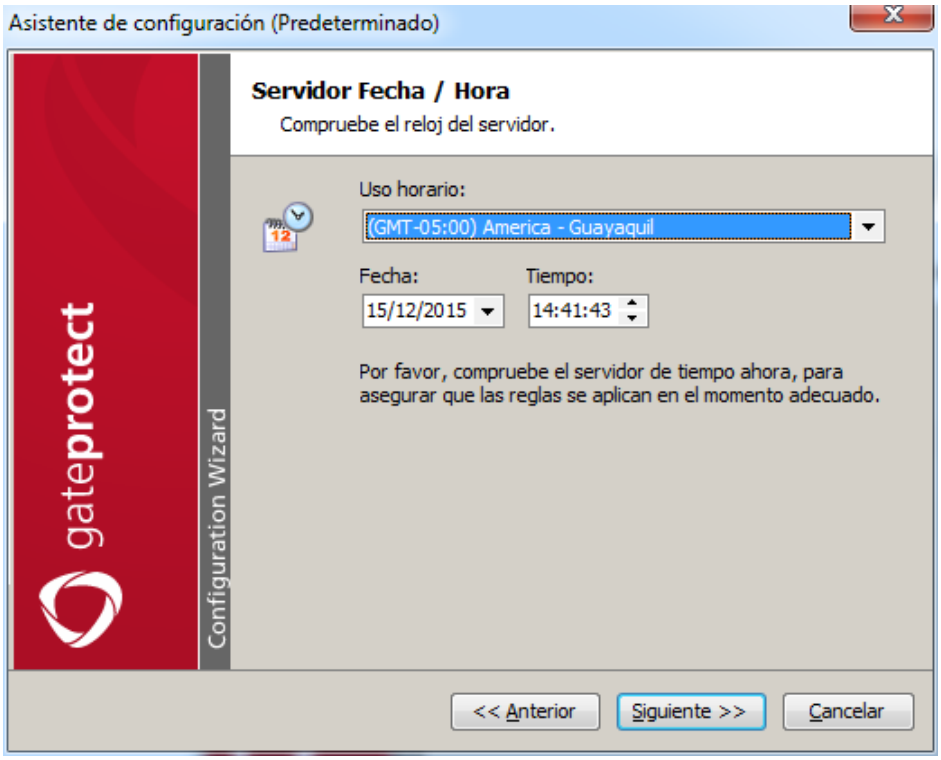
3. Ingresar el usuario y contraseña del servidor. Por defecto Usuario: admin Pass: admin



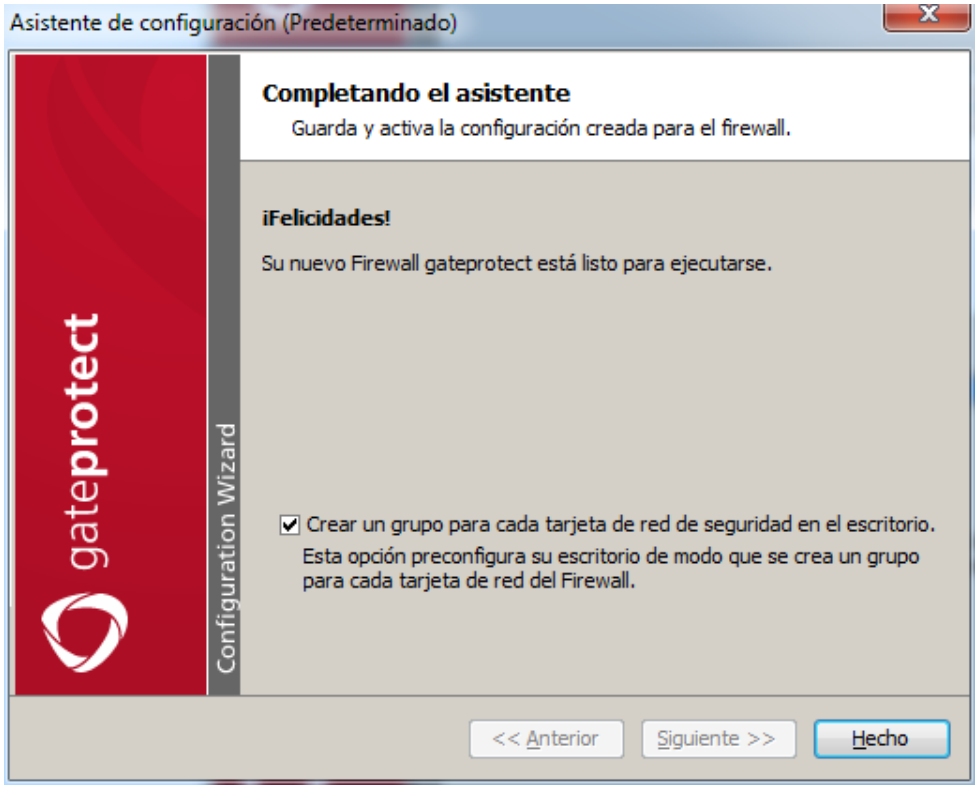
4. En la siguiente ventana dejar marcada la opción por defecto y presionar Siguiente.

5. Cambiar la contraseña por defecto del administrador.

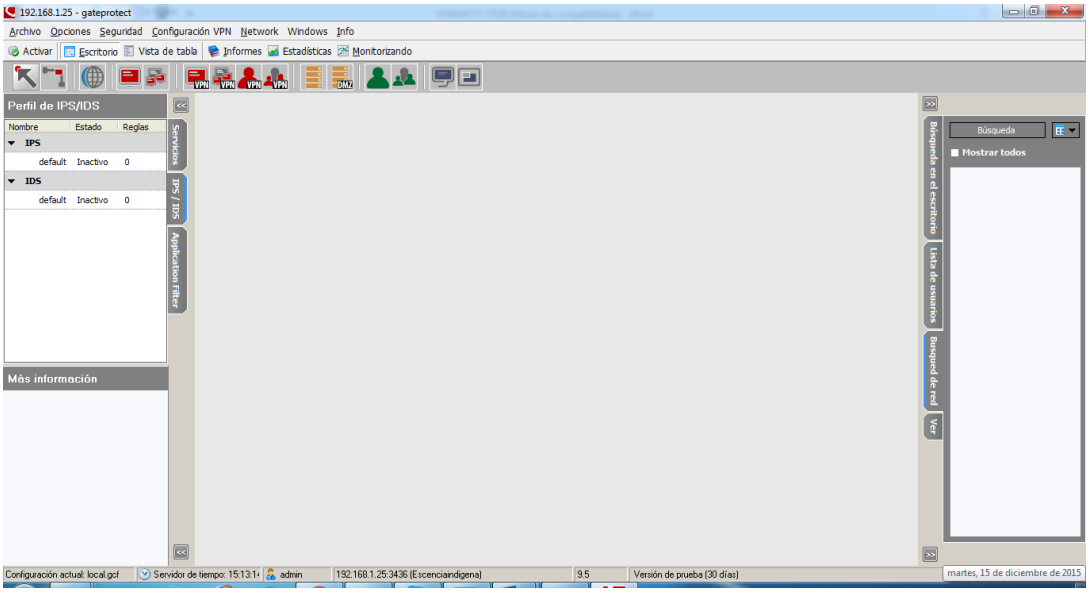
6. Seleccionar la fecha y hora correcta y presionar Siguiente.



7. Se ha completado la instalación. Presionar en Hecho.



8. Aparece el escritorio de administración del servidor en el cual ya se puede empezar a trabajar.



ANEXO 6: SUMMARY

SUMMARY

This project presents a management system for perimeter security and access distribution network of the saving and credits Cooperative Escencia Indígena Ltda. Ibarra, based on the ISO 27002:2013 norm.

It was started with the theoretical Foundation related with the themes about information security, cyber-attacks, methods and tools to combat them. The institution was visited in order to identify its technology infrastructure, identify risks and vulnerabilities, and find a solution.

The handbook of policies and good practices of information security was made based on Objectives controls and checkpoint of the ISO / IEC 27002: 2013 applicable to the problems and needs found in the technological infrastructure at last users level and in the distribution layer of the institution.

An equipment Gate Protect GPA 500 was purchased and installed because it has all the features for the proposed design and includes a firewall, DMZ and IDS / IPS, moreover of features such as spam controlling, viruses and others.

Finally, the analysis of the cost of equipment that used in the design was made in order to know the project investment. Also, the conclusions and recommendations obtained in the project was written.